

TRADOC Guide for the Publicly Accessible Web: a Handbook for “Survivors”

**Version 2.0
August 2009**

**A compendium of policy, guidance,
recommendations, and best practices for
public-domain Web content**



TRADOC Guide for the Publicly Accessible Web: a Handbook for “Survivors”

**Prepared by TRADOC Public Affairs Office
Bldg. 27, 66 Ingalls Road
Fort Monroe, VA 23651
(757) 788-3463 (DSN 680)**

**Contact: TRADOC Web Content Manager,
lisa.alley@us.army.mil**

Table of Contents		
Chapter 1: Overview		7
	The public domain and DoD's principles of information vs. protection of information	7
	The foundation of this <i>Guide</i> : the TRADOC Web Content Review Program	11
	Roles: content provider, content reviewer, content manager	15
Chapter 2: The content provider		20
	The content provider's role in the organizational Website	20
	Writing for the Web: it's a strategy	20
	Writing for the Web: style	22
	Content providers and the review process	24
	General military requirements	26
	Graphics / images / multimedia guidelines	27
	PAO as content provider	29
	TRADOC pre-dissemination content review procedures checklist	31
Chapter 3: Content reviewers / the content review		33
	Personally identifiable and subject to the Privacy Act	33
	Classified according to the National Security Act	35
	Subject to a FOIA exemption	35
	Otherwise "sensitive"	40
	The special problem of PII	40
	Roles and responsibilities for reviewers	48
	Reviewer roles and responsibilities: organizational Webmaster	49
	Reviewer roles and responsibilities: OPSEC officer	49
	Reviewer roles and responsibilities: security manager	57
	Reviewer roles and responsibilities: SJA	58
	Reviewer roles and responsibilities: QI Program reviewers	59
	Reviewer roles and responsibilities: PAO	62
	TRADOC review steps	64
	Execution	67
	Policy violations	68
	The WCWG	70
	Post-dissemination reviews	71
	Webmaster review procedures checklist	72
	Policy review checklist	74

	OPSEC / security review checklist	84
	Legal counsel's review checklist	91
	QI review checklist	93
	PAO review checklist	94
	Loss-of-PII consequence table	107
	Releasability checklist	108
Chapter 4: Web-content managers / Web-content management		126
	Organizational Website coordinator	126
	Post or ACOM Web-content manager	127
	Web manager vs. Web-content manager	130
	General federal requirements	134
	When to use AKO, when not to	137
	"Strategic Webbing"	140
	Public accessibility and Web security	152
	Social media	158
	Webpage design and content formatting	169
	Policy: content limitations	170
	Policy: required content	172
	Policy: Section 508 compliance	176
	Policy: other policy and guidance	180
	Policy: installation newspapers on the Web	181
	Website coordinator / Web-content manager checklist	185
Chapter 5: Record-keeping and file management		190
	Web files management	191
	Electronic-records management	191
Chapter 6: Required and recommended training		193
	Mandatory Web training	193
	Elective / recommended OPSEC training	194
	Public Affairs professional training	194
	IT / IA professional training	195
	Other OPSEC recommendations	195
Summary		196
Appendix A: References		197
	Clearance / release of information	197
	Freedom of Information Act	197
	Information quality	198
	Miscellaneous	198

	Policy and guidance, Web	199
	Privacy / personal information	200
	Public Key Infrastructure	200
	Records and file management	201
	Section 508	201
	Security / operations security	201
Appendix B: Glossary		204
	Section I: Acronyms	204
	Section II: Definitions	208
Appendix C: Key management controls checklist	(Required by AR 25-1)	237
Appendix D: Required notices		239
	DoD standard privacy and security notice	239
	DoD standard cookie disclaimer	240
	DoD standard external-links disclaimer	240
	DoD standard access-control notice and consent banner	241
	DoD PA / PAS statements	241
	DoD Platform for Privacy Preferences Project notice	243
Appendix E: Examples of critical information		244
Appendix F: Examples of CUI		250
Appendix G: Examples of FOUO information		251
Appendix H: Examples of OPSEC indicators		256
Appendix I: Examples of sensitive information		260
Appendix J: Consolidated list of PII		263
Appendix K: DoD mandated information-posting process		265
	Paragraph 3, Part II, DoD Web policy	265
	DoDD 5230.9	268
	DoDI 5230.29	270
Appendix L: Templates for required content		275
	Website purpose statement and plan	275
	Organization mission and outline of structure	276
	Other required statements	282
	Public policy on hyperlinks	282
	External-links disclaimer	284
	“Important Notices” page	284
	“Contact Us” page	286
	“About Us” page	287
	Sitemap	287
	FAQ page	287

	“Help” page	287
	Search page or box	288
Appendix M: Writing for the Web		289
	The basic principles	289
	News values	289
	Readability	290
	The inverted pyramid	291
	Content’s natural parts	292
	Common mistakes	292
Appendix N: Section 508 compliance standards		294
Appendix O: Measuring the success of your publicly accessible Website and social-media engagements		297
	Best practices and lessons-learned	297
	Quantifying data	299
	The annual survey / user assessment	306
Appendix P: IO and Public Affairs		310

Chapter 1 Overview

The *TRADOC Guide for the Publicly Accessible Web* is primarily for Web-content providers, Web-content reviewers, and Web-content managers, to enable them to “survive” the sheer amount of federal, Department of Defense (DoD), and Department of the Army (DA) Web-content policy – policy that sometimes presents “landmines” because it doesn’t seem to agree. The *Guide*’s major target audience is Public Affairs personnel who support U.S. Army Training and Doctrine Command (TRADOC) centers of excellence (CoE) and individual schools, but other professional disciplines are included to bring together all the various policies and guidance on the Web portion of the public domain, to synchronize it and clarify it where possible, and to provide tools for Public Affairs Offices (PAOs) and TRADOC content providers / content reviewers to use. The *Guide* stresses “how to do” something as well as discusses content prohibitions to help guide PAOs in their decision-making during their content review and approval processes. The *Guide* also can be used to establish best practices and benchmarks.

It’s important to understand from the outset that the *Guide* is a user guide – it isn’t directive – but the policy it cites *is* directive and sometimes punitive, as in the case of non-compliance to Army Regulation (AR) 530-1, AR 25-1, or AR 25-2. So an important secondary aim of the *Guide* – in addition to policy synchronization and assistance with tools – is simply awareness.

Some “admin” notes for users of the *Guide*:

- Citations of references are provided via footnotes throughout the *Guide*. These references, and other federal, DoD, DA, and TRADOC policy and guidance touching on publicly accessible Websites / Webpages, are listed in Appendix A.
- Important points, principles, concepts, and references will be **highlighted** throughout the *Guide* for “scanners” of this information, to aid comprehension and speed of reading.
- Policy and guidance published subsequent to this *Guide* will be included in the *Guide*’s next version.¹ Please send notification of any policy and guidance changes to lisa.alley@us.army.mil.
- Most references included in this *Guide* are available on-line (Web addresses where available are included in Appendix A), and are also included in the Headquarters (HQ) TRADOC Web Content Working Group (WCWG)’s portal on Army Knowledge On-line (AKO). If a user is not registered for the TRADOC WCWG portal but wishes access, contact the portal administrator at lisa.alley@us.army.mil.
- TRADOC PAO is the publisher of this *Guide* as TRADOC’s Web Content Manager and Executor.² TRADOC PAO recommends that you use this *Guide* in conjunction with TRADOC Regulation (TR) 25-1, available on the TRADOC Website, <http://www.tradoc.army.mil/tpubs/regndx.htm>, to receive a clear picture of the technical issues and requirements. Most technical requirements, except for access control and the requirements for Section 508 compliance, are not within the scope of this *Guide*.
- Policy and guidance questions not addressed by this *Guide* may be brought to the attention of the TRADOC Web Content Manager, lisa.alley@us.army.mil. Operations security (OPSEC) questions should be referred to your organizational OPSEC officer.

THE PUBLIC DOMAIN AND DOD’S PRINCIPLES OF INFORMATION VS. PROTECTION OF INFORMATION

We’ll start by reviewing some foundational concepts. First, we mentioned the “public domain” above – what is it and how does it apply to the Web?

We’re not speaking here of “public domain” when that phrase is defined as intellectual property that isn’t owned or controlled by anyone via copyright, trademark, or other methods, but belonging to all people in general – aka “the public.” Nor are we speaking of public domain in terms of property or land. We *are* speaking of information in the public domain. Since the public raises the military via constitutional provision, pays for its operation via taxes, and therefore essentially “owns” it, **all official information that DoD employees produce belongs to the public, unless the information is specifically exempted from release into the public domain.** DoD’s overarching framework for its Websites must be likewise: to provide U.S. citizens information on the military entities they support with their taxes,

¹ An annual update cycle is currently planned.

² TRADOC memorandum, “TRADOC Public Website Content Management,” June 11, 2009.

and to support the democratic process as a whole. Federal-agency public Websites are considered “information-dissemination products” as defined by Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources.”³ Therefore TRADOC public Websites must be managed as an information resource not primarily for the military, but for the public. Federal Websites, including the military’s, are required by law to follow the guidance in OMB Circular A-130, “Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies” (67 Code of Federal Regulations (CFR) 5365), OMB memorandum M-05-04, and other information-policy issuances.

Official DoD information, per DoD Directive (DoDD) 5230.9, is information in DoD’s custody and control; information that relates to information in DoD’s custody and control; or information that was acquired by DoD employees as part of their official duties or because of their official status within DoD.

Sometimes this is hard for us to get our arms around, but our commanders don’t actually “own” the Website. To reiterate, our public Websites are actually owned by American taxpayers, so we owe it to them to deliver the very best quality we can on the products we offer them on the Web – and, furthermore, to offer Web products they’ll find relevant. This is why Public Affairs must take the lead on Web content: to balance the public domain, strategic messages, an organization’s wishes, and the commander’s intent – this balance is an art, not a strict interpretation of black-and-white policy.

Information as public property. The President’s approach is that information is a “national asset.”⁴ As AR 25-1 states, information produced by Army employees is a shared resource and should be available to everyone except where release of it is restricted for reasons of national security, privacy, sensitivity, or proprietary rights.⁵ However, there is also a limitation to AR 25-1’s conceptual framework in that it views information as a commodity to be managed in terms of collection, processing, and storage – of course, a very net-centric viewpoint. And therefore its definition of a public Website is framed completely by what sort of network security exists – to wit, **AR 25-1 defines a public (or publicly accessible) Website as an Army Website with access unrestricted by password or Public Key Infrastructure (PKI) authorization,⁶ while a non-public Website is an Army Website with access restricted by password or PKI user authorization.** In fact, the alternate term AR 25-1 uses to define a public Website (“publicly accessible”) is very telling – the concept of a public Website is shaped by access control, or lack thereof. This *Guide* offers a different conceptual framework: that of knowing what isn’t releasable so that everything else relevant to the public is released. In fact, if the term *publicly accessible* “went away” and was replaced by a term like *public-facing* – or, more simply, *public* – that would be more accurate and more in spirit with the actual reasons our Internet Websites should exist.

A Website is one of the major tools Public Affairs has to meet its responsibilities, per AR 360-1, to fulfill the Army’s obligation to keep the American people and the Army informed, and to help establish the conditions that lead to confidence in America’s Army and its readiness to conduct full-spectrum operations.⁷ An attitude of non-transparency (as opposed to President Barack Obama’s commitment that the government will operate under “an unprecedented level of openness”)⁸ will not engender public confidence, nor will it aid the Army’s recruiting efforts. Therefore we must educate ourselves to think in terms of releasing information unless the information strictly meets the definition of “non-public” information.

It is strange that AR 25-1 – an information-technology (IT) regulation and not a Public Affairs one – contains the Army’s only definition of “public domain” and its antithesis, the “non-public” domain. (See Paragraph 1-7, AR 25-1.) For information to be exempt from release to the public – in other words, to be non-public information, the information must meet one of these stipulations:

- Personally identifiable and subject to the Privacy Act;
- Classified according to the National Security Act;

³ See OMB memorandum M-05-04, “Policies for Federal Agency Public Websites,” Dec. 17, 2004.

⁴ “Transparency and Open Government” memo, Jan. 21, 2009.

⁵ Paragraph 1-7, AR 25-1.

⁶ Section II of glossary, AR 25-1. See also ALARACT “Website Security Policy Compliance,” Dec. 19, 2008.

⁷ Paragraph 1-6, AR 360-1.

⁸ “Transparency and Open Government” memo. Per Obama’s memo, transparency will engender public trust, participation and collaboration; strengthen the democracy; and promote accountability, efficiency, and effectiveness in government.

“The importance of the Internet has grown exponentially over the last decade, but the government’s ability to provide on-line services to the American people hasn’t grown at the same pace. ... [W]hen the [American people] need government information and services on-line, they [should] be able to easily find relevant, accurate, and up-to-date information; understand information the first time they read it; complete common tasks efficiently; get the same answer whether they use the Web, phone, email, live chat, read a brochure, or visit in-person; provide feedback and ideas and hear what the government will do with them; [and] access critical information if they have a disability or aren’t proficient in English. ... The Web can foster better communication and allow people to participate in improving the operations of their government. By listening to our customers, we can provide better services, focus on their most pressing needs, and spend their tax dollars efficiently. ... [I]nvest in the Web as a strategic asset and make these goals a reality.” – **Putting Citizens First: Transforming On-line Government**, Federal Web Managers Council whitepaper

- Subject to a Freedom of Information Act (FOIA) exemption; or
- Otherwise “sensitive.”

This *Guide* will include more details on these stipulations in following chapters and will also discuss For Official Use Only (FOUO) information, which is specifically defined as information that comes under one of the FOIA-exempt categories and is unclassified.⁹

Non-public information may be shared for official purposes within DoD and with other government agencies affiliated with DoD’s contracts or operations, keeping in mind any stipulated access and release restrictions. Non-public, official Army information may be posted for authorized individuals to AKO¹⁰ or other approved controlled-access Webserver – as discussed in Chapter 4, the controlled access makes the Webserver, and the information thereon, private. Private information requested by private-sector individuals or organizations should be referred to the local FOIA officer to determine whether it’s releasable.¹¹

By contrast, public-domain information is not only government-owned but is also not personally identifiable, classified, subject to a FOIA or Privacy Act exemption, or otherwise considered to be sensitive. The Army is bound to either routinely make this information public or to provide the information upon public request. Army personnel should find reasons to release information rather than reasons to not release information in the spirit of the FOIA (see Paragraph 1-300, AR 25-55); in accordance with (IAW) Paragraph 5-5b, AR 360-1, information that would be released if requested under the FOIA anyway should be released publicly when requested through Public Affairs channels – this avoids invoking the FOIA and provides timely information to the public.

In contrast to non-public information, public-domain Army information may be posted on an Army public Website.

Recalling our statement that “we must educate ourselves to think in terms of releasing information unless the information strictly meets the definition of ‘non-public’ information,” TRADOC PAO isn’t living in a “dream world” regarding releasing information; quite the opposite – we know that management of Web content isn’t as cut-and-dried as “release everything.” (The war on terrorism has made everyone so cautious that many organizations approach Web content from the “zero-based” perspective – discussed in Chapter 4 – and so we’re advocating that the Army as a whole begin a process of re-education to think in terms of “why not” release information rather than “why” release information.) We emphasize that **TRADOC public Websites¹² are critical in providing information to various target audiences, but their use also incurs a significant responsibility for the information provider.** (See Chapter 2.) The Web’s popularity has grown exponentially because of its accessibility just about anywhere in the world and the rapidity with which information can be released on it – and the Web’s popularity within DoD is projected to continue. Experts estimate that, in the near future, most unit data exchange will be via Internet

⁹ Paragraph 1-7, AR 25-1.

¹⁰ See Paragraphs 6-7c(3) and 6-7d(1), AR 25-1. In fact, these references state that non-public, official Army information *will* be posted on AKO, and that private Websites separate from AKO can be established only when AKO can’t support requirements.

¹¹ Paragraph 1-7, AR 25-1.

¹² A Website in which content is developed and maintained by, or at the request of, a TRADOC activity or subordinate organization, as defined by TRADOC G-6 (email from TRADOC Webmaster Nov. 20, 2006).

Websites.¹³ The Federal Web Managers Council estimates that there are about 24,000 U.S. government Websites on-line (but caveats this by saying that no one knows the exact number of Websites Uncle Sam has).¹⁴ However, the power of the Web creates a tension between the need to disseminate information and the need to protect it. It creates tension between DoD's principles of information¹⁵ and DoD's policy that an individual's privacy is a "personal and fundamental right that shall be respected and protected,"¹⁶ for instance. (See the discussion on personally identifying information (PII) in Chapter 3.) The issue of PII creates a sort of schizophrenia in our practice of releasing information, as PII involves the heart of Public Affairs functions and activities – part of PAO's mission is to tell the Army's story, and the Army is people.

The need to disseminate information. Our national leaders have determined that sincere, direct communication is critical to our national success. America is an open, democratic society. Our candid approach to media coverage of military actions – in spite of the attendant danger of sensitive-information release – is because media coverage, to a large extent, will shape domestic and international public perception of the national-security environment now and in the years ahead. Besides our responsibility to the American public, we are responsible for informing our own internal target audience. Commanders and their PAOs can use the Web to tell the Army story and to correct disinformation / distortions as quickly as possible.

The need to protect information. On the other hand, we give away too much; this has been evident for several years. Irresponsible Web-content postings during the last few years have put Soldiers at risk. As former Secretary of Defense (SECDEF) Donald Rumsfeld said in a Jan. 14, 2003, memorandum on Website OPSEC discrepancies, our adversaries avidly glean information from our Websites: "An Al-Qaeda training manual recovered in Afghanistan states, 'Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of information about the enemy.' ... One must conclude our enemies access DoD Websites on a regular basis. The fact that [FOUO] and other sensitive unclassified information ... continues to be found on public Websites indicates that too often data posted are insufficiently reviewed for sensitivity and / or inadequately protected." Further, while many of us understand that plans and capabilities information is most likely FOUO, and posting this information to a public Website is most likely an OPSEC violation, we all don't understand that PII can be FOUO and an OPSEC violation, too – although this was determined early in the war on terrorism.¹⁷

In the zero-based approach to Web content, instead of vetting content for words, phrases, sentences, or photographs that may be targets for an adversary, organizations determine what information is **strictly necessary** to post on public Websites to fulfill their mission, and then post all other content on non-public domain venues. This approach holds that there is no sure way of identifying those items – which, when placed in conjunction with information from other sites or sources – may become critical OPSEC indicators. The zero-based approach to Web content is recommended by security experts because every Army organization produces or has information that ultimately affects the ability of U.S. forces to accomplish missions, and every organization must identify and protect this information.

¹³ Paragraph E-5, AR 380-5.

¹⁴ *Putting Citizens First: Transforming On-line Government*, Federal Web Managers Council whitepaper, November 2008.

¹⁵ The DoD principles of information are listed in Enclosure 2, DoDD 5122.5, and Appendix H, AR 360-1. Summarized here, those principles are: "It is DoD policy to make available timely and accurate information so that the public, Congress, and the news media may assess and understand the facts about national security and defense strategy. Information will be made fully and readily available, consistent with the statutory requirements, unless its release is precluded by current and valid security classification. The provisions of the [FOIA] will be supported in both letter and spirit. ... Information will be withheld only when disclosure would adversely affect national security, threaten the safety or privacy of the men and women of the armed forces, or if otherwise authorized by statute or regulation." Also see Paragraph 4c, DoDD 5230.9: "The public release of official DoD information is limited only as necessary to safeguard information requiring protection in the interest of national security or other legitimate governmental interest." And Paragraphs 4, 4.1, and 4.3, DoDD 5200.1: "It is DoD policy that national-security information will be ... safeguarded, [IAW] national-level policy issuances. ... The volume of classified national-security information will be reduced to the minimum necessary to meet operational requirements."

¹⁶ Paragraph 4, DoDD 5400.11.

¹⁷ Three DoD-level memorandums issued Oct. 18, 2001, Nov. 9, 2001, and Dec. 28, 2001, established this. The Oct. 18 memo from the DEPSECDEF, "Operations Security Throughout the Department of Defense," states that "[m]uch of the information we use to conduct DoD's operations must be withheld from public release because of its sensitivity." The Nov. 9 memo from the Director, Administration and Management, "Withholding of Personally Identifying Information Under the Freedom of Information Act (FOIA)," cites the DEPSECDEF's memo as emphasizing "the increased risks to U.S. military and civilian

DoD policy is to provide accurate and timely information (“maximum disclosure with minimum delay”) consistent with the requirement to maintain OPSEC, protect intelligence information and sources, and protect the welfare and privacy rights of Soldiers, patients, next-of-kin, and family members. All personnel, including PAOs, are charged to “practice security at the source.”

Beyond protecting information, DoD and Army policy require each Website / Webpage or publicly accessible portal page to have a “verified valid mission” need to disseminate the information contained on the site / page.¹⁸ Army Chief Information Office (CIO) / G-6 guidance is that “[o]nly official Army information that is releasable and of value to the public may be posted on Army public Websites.” These approaches are based on the “zero-based content” conceptual framework, where information is released *if* it meets standards and exceptions, and is the antithesis of Public Affairs practice and the spirit of the FOIA. However, zero-based content is a favorite practice with, understandably, information-assurance (IA), IT, and OPSEC practitioners, and therefore Public Affairs must be deeply involved in Web content to ensure that the public’s information is released to it, while information that *must be* protected, is.

THE FOUNDATION OF THIS GUIDE: TRADOC WEB CONTENT REVIEW PROGRAM

There’s really only one solution to balance the “clash of cultures,” better manage risk, and ensure that Websites provide quality information: a robust Web Content Review Program¹⁹ with an appointed Web-content manager and Website coordinators. (The Web-content manager / Website coordinator will be discussed more in Chapter 4.) HQ TRADOC’s content-review measures were recognized by Army G-3/5/7 as a “best practice” in 2005, but even our current program could be enhanced IAW this user guide. Content review is not censorship,²⁰ as some organizations view it; in the end, a strong review program will not only help protect our Soldiers but will also better provide top-quality customer service to Website users.

TRADOC’s Web Content Review Program – established IAW DoD policy and AR 25-1, and in response to a DoD Inspector General (IG) report²¹ – is not only TRADOC’s response to DoD and Army requirements for a content-review program as well as to the requirements of an Army at war, but it also balances the needs of dissemination vs. protection of information, and is the foundation of the principles in this *Guide*.

personnel, DoD operational capabilities, facilities and resources”; says that the change in security posture affects DoD’s policies for implementing the FOIA; and applies more restrictions for releasing PII. The Dec. 28 memorandum from the ASD-C3I, “Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites,” builds on the Oct. 18 and Nov. 9 memos and states that PII “regarding all DoD personnel may be withheld by the [DoD] components under exemption (b)(6) of the FOIA. ... This action makes the information which may be withheld FOUO and inappropriate for posting to most unclassified DoD Websites.” This latter memo directs PII on all DoD personnel “now eligible to be withheld under the FOIA” per the Nov. 9 memo to be removed from publicly accessible Webpages and Webpages with access restricted only by domain or IP address, applicable to unclassified DoD Websites regardless of domain or sponsoring organization. This memorandum, which is still in effect, requires removal of “name, rank, email address, and other identifying information regarding DoD personnel, including civilians, active-duty military, military family members, contractors, members of the National Guard and Reserves, and Coast Guard personnel when the Coast Guard is operating as a service in the Navy.” See Chapter 3 for further discussion on PII, including exceptions to this policy.

¹⁸ Enclosure 5, DoD Manual 5205.02-M; SECDEF message, “Website OPSEC Discrepancies,” Jan. 14, 2003; Paragraph 6-7c(3), AR 25-1; ALARACT “Website Security Policy Compliance,” Dec. 19, 2008; Paragraph 5b(5)(a), TRADOC OPSEC Plan. Also see Paragraph 3-5a(1), AR 360-1: a Public Affairs publication may be established only when a “valid mission requirement” exists – although this traditionally applies to installation newspapers, Web publishing also comes under the definition for Public Affairs publications.

¹⁹ DoD and Army policy very clearly require a deliberate process for reviewing and clearing Web content. See Pages 13-14 and Chapter 3. Other policies are included in the Web-content review team chart. This *Guide* elaborates on the review program established at HQ TRADOC in 2005 (and enhanced as subsequent DoD and Army policy and guidance has been issued) as the Web-content oversight mechanism for the command.

²⁰ See Paragraph 6-7c, AR 360-1.

²¹ The DoD IG’s report of June 5, 2002, in criticizing TRADOC’s Web-content review process, noted that “[t]he approval process for posting information on Websites is necessary to ensure that only properly cleared information is released to the general public on Army Websites. Although Web policy is the responsibility of the [G-6], the release of information is the responsibility of the Chief of Public Affairs. Accordingly, the Chief of Public Affairs, in coordination with the [G-6], must establish an oversight mechanism to monitor whether Army organizations are using consistent procedures for reviewing and approving all information posted to Websites.”

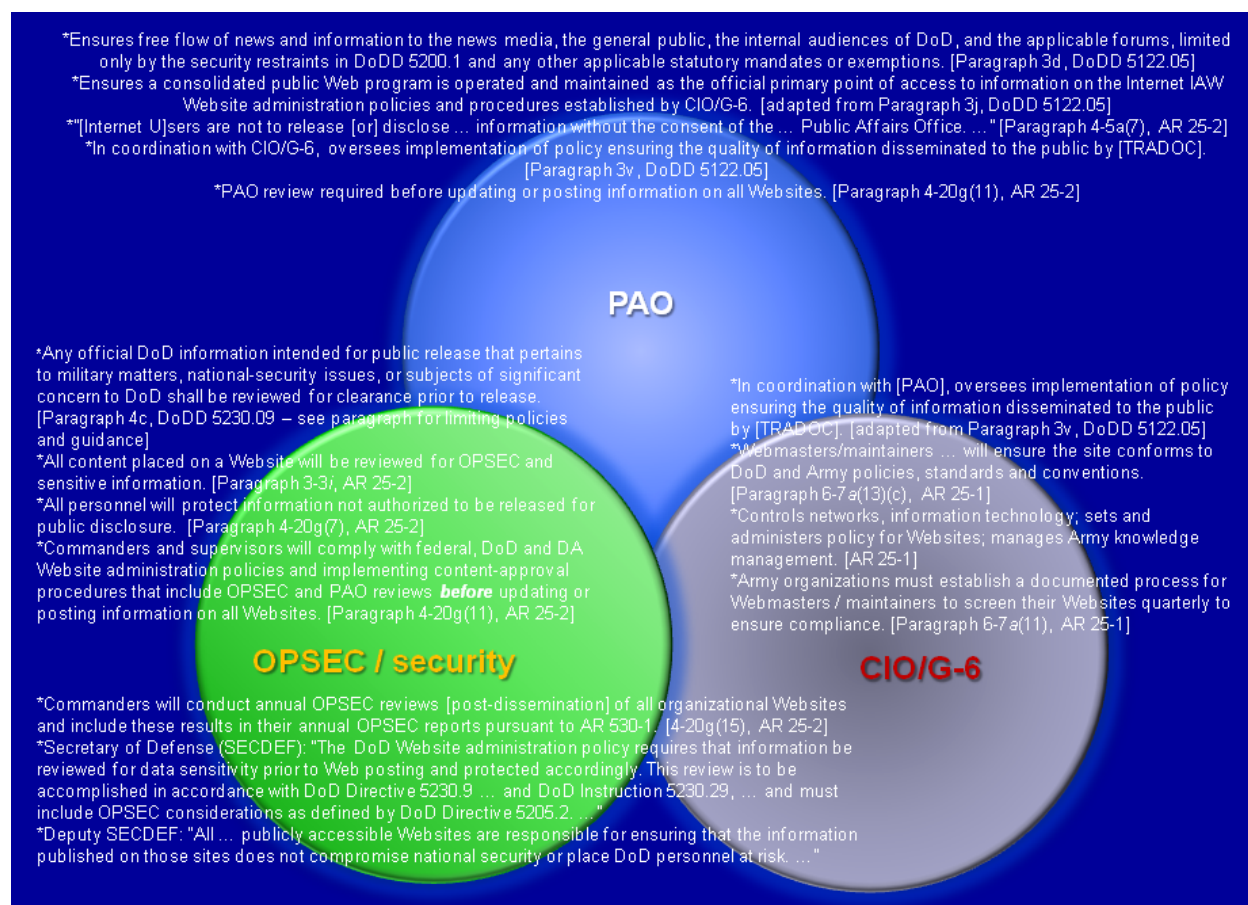


Chart 1-1. The Web Content Review Program team, which has mandated responsibilities and requirements for Web-content screening and clearance.

The TRADOC Web Content Review Program rests on the principle that the primary triad of OPSEC, G-6, and PAO experts²² work as a team to safeguard information, yet still ensure that “accurate and timely information is made available to the public and the Congress to help the analysis and understanding of defense strategy, defense policy, and national-security issues.”²³ All team members fulfill DoD and Army mandates. (See illustration above.) All team members seek a consensus that is mindful of the guidance contained in the Deputy Secretary of Defense’s (DEPSECDEF) memorandum on information vulnerability and the Worldwide Web (WWW): “[Leaders] assume a management responsibility that extends beyond general Public Affairs considerations regarding the release of information into the realm of [OPSEC] and force protection, [and] ... must enforce the application of comprehensive risk-management procedures to ensure that the considerable mission benefits gained by using the Web are carefully balanced against the potential security and privacy risks created by having aggregated DoD information more readily accessible to a worldwide audience.”²⁴

TRADOC’s Web Content Review Program incorporates clearance-review procedures IAW DoDD 5230.9 and Department of Defense Instruction (DoDI) 5230.29 for official DoD information.²⁵ (See Chapter 3 and Appendix K.) The program also requires those who take part in it to be trained, knowledgeable experts such as OPSEC and

²² This idea of a “primary triad,” although implemented at HQ TRADOC in 2005, is supported by ALARACT “Website Security Policy Compliance,” Dec. 19, 2008, which directs the personnel who “operate and review” Websites (PAOs, Webmasters / maintainers, and OPSEC or IA specialists) to complete “mandatory” OPSEC training. The ALARACT’s operator / reviewer categories square with the PAO, G-6 (Webmasters / maintainers), and OPSEC / IA divisions of the chart above.

²³ Paragraph 4a, DoDD 5230.9.

²⁴ Memorandum from the DEPSECDEF, “Information Vulnerability and the Worldwide Web,” Sept. 24, 1998. Also quoted in AR 380-5; see the Summary in this *Guide*.

²⁵ Paragraph 3.5.1, Part II, *DoD Website Administration Policy and Procedures* (hereafter referred to as the DoD Web policy).

security practitioners – familiar with the rules governing FOUO information as well as pertinent security classification guides (SCGs) – and quality of information (QI) experts, IAW DoD Web policy. The OPSEC and security experts should also be familiar with the aspects of their organization’s operations considered critical; their organization’s vulnerabilities; and the pertinent threat so they can properly assess the nature of the risk associated with posting specific information to public-domain Websites.²⁶

You may be thinking, “That’s great for HQ TRADOC; I have other things to do besides deal with Web content. And **who / what says I *must* have a Web Content Review Program, and that I *must* do all this reviewing before people post information to Websites, and that I *must* review information after it’s posted, too?**” Fair-enough question; **here’s the answer as to who / what:**

- Paragraph 3.5.1, Part II, DoD Web policy: “DoD components must establish, [IAW] [DoDD] 5230.9 and [DoDI] 5230.29..., clearance-review procedures for official DoD information that is prepared by or for DoD personnel and is proposed for posting to publicly accessible Websites.”
- Paragraph 2, Part V, DoD Web policy: “All information proposed for posting to a publicly accessible Website must be reviewed IAW the provisions of DoDD 5230.9 and DoDI 5230.29, and as described in Paragraph 3, Part II, of the DoD Web policy.” (A breakdown of DoDD 5230.9, DoDI 5230.29, and Paragraph 3, Part II, of the DoD Web policy is available in Appendix K.)
- Paragraph 4b, DoDD 5230.9: “It is DoD policy that ... [a]ny official DoD information intended for public release that pertains to military matters, national-security issues, or subjects of significant concern to [DoD] shall be reviewed for clearance **prior to** release.”
- Enclosure 5 (information-protection requirements), DoD Manual 5205.02-M: “This section supplements guidance related to the release of information in DoDD 5230.09, [DoDI] 5230.29 and [the DoD Web policy]. ... The OPSEC program manager or coordinator will work closely with [PAO], information security, Web administrators and other officials. ... Commanders and directors are responsible for ensuring ... that review procedures are implemented [and shall] develop, establish, and implement policies and procedures to deny adversaries the opportunity to take advantage of publicly available information, especially when aggregated.”
- Paragraph 6-7a(11), AR 25-1 [specific to personal-privacy screening]: “Army organizations must observe [f]ederal, [DoD], and Army policies for protecting personal privacy on official Army Websites and must establish a documented process ... to **screen their Websites quarterly** to ensure compliance.”
- Paragraph 6-7c(3), AR 25-1: “Army commanders / organizational heads will ensure that the PAO and other appropriate designee(s) (for example, command counsel, force protection, intelligence, and so on) review and clear Web content and format **prior to** posting to the Internet. Information contained on publicly accessible Websites is subject to the policies and clearance procedures prescribed in AR 360-1, Chapter 5, for the release of information to the public.”
- Paragraph 6-7c(4), AR 25-1: “The designated reviewer(s) will conduct routine reviews of Websites on a **quarterly** basis to ensure that each Website is in compliance with the policies herein and that the content remains relevant and appropriate. The use of Web-analysis software for reviews is encouraged but not required.”
- Paragraph 4-20g(11), AR 25-2: “Commanders and supervisors will comply with [f]ederal, [DoD], and DA Website administration policies and implementing content-approval procedures that include OPSEC and PAO reviews **before updating or posting** information on all Websites.”
- Paragraph 5-1, AR 360-1: “[DoD] policy requires any official information intended for public release that pertains to military matters, national security issues, or subjects of significant concern to the DoD be cleared by appropriate security review and [Public Affairs] offices **prior to** release. This includes materials placed on the Internet or released via similar electronic media.”
- Paragraph 6-1b, AR 360-1: “Clearance, through security review and [Public Affairs] channels, is required for all official ... writings that are presented or published in the civilian domain, to include materials placed on the Internet or released via similar electronic media.”
- DEPSECDEF memorandum, “Department of Defense (DoD) Website Security Policy Compliance,” Sept. 25, 2008: “Each [organization] is required to have processes in place that ensure all information posted to

²⁶ Paragraph 3.5.2, Part II, DoD Web policy.

publicly accessible Websites is reviewed and approved **prior to** posting. This process includes review of content for sensitivity, including specifically identifying [FOUO] information, and appropriate distribution / release controls. Each [organization] is responsible for ensuring the process to accomplish these reviews is consistently applied.”

- DEPSECDEF memo cited in All Army activities (ALARACT) message “Website Security Policy Compliance,” Dec. 19, 2008: “[T]he DEPSECDEF require[s] components to certify their implementation of a review and approval process for all information posted to publicly accessible Websites. ... Army policy requires all organizations to appoint qualified individuals ([PAOs] and / or others) to properly clear information **prior to** posting it on their respective Websites and to **conduct quarterly reviews** of Website content. The quarterly evaluation includes format, required content restrictions and inclusions, privacy, and [OPSEC].”
- The Secretary of the Army (SecArmy)’s executive-summary response to the DEPSECDEF’s tasking in “Department of Defense (DoD) Website Security Policy Compliance”: “Army policy requires all organizations to appoint qualified individuals ([PAOs] and / or others) to properly clear information **prior to** posting it on their respective Websites and to **conduct quarterly reviews** of Website content. The review includes format, required content restrictions and inclusions, and privacy and [OPSEC] considerations per the Website-management control checklist in AR 25-1 (Appendix C).”
- All DoD activities (ALDODACT) message 11/06, “Information Security / Website Alert,” Aug. 9, 2006 (referred to in DEPSECDEF memo of Sept. 25, 2008): “Effective immediately, no information may be

“Agencies should be required and funded to conduct regular content reviews, to ensure their on-line content is accurate, relevant, mission-related, and written in plain language. They should have a process for archiving content that is no longer in frequent use and no longer required on the Website.” – **Putting Citizens First: Transforming On-line Government**, Federal Web Managers Council whitepaper

placed on Websites that are readily accessible to the public **unless it has been reviewed** for security concerns and approved [IAW] [DEPSECDEF] memorandum, ‘Website Policies and Procedures,’ Dec. 7, 1998 [the DoD Web policy’s cover memorandum] and, as applicable, [DoDI] 5230.29, ‘Security and Policy Review of DoD Information for Public Release.’ Command review procedures must also specifically address identification of [FOUO] information and shall ensure all information is reviewed by personnel trained in [OPSEC].”

The **clearance program must include multimedia and visual information (VI)**, reviewed both before and after completion of the product. For example:

- Paragraphs 7-7a(6)(b)10, 12 and 18, AR 25-1: “The VI production activity ... will obtain a legal review and public-release clearance **prior to** production distribution. (Legal review and public-clearance documents will be maintained throughout the lifecycle of the production.) **Prior to** commitment of production funds for a product whose intended audience is the public, a copy of the treatment or script will be submitted, with legal determination, to Public Affairs requesting public exhibition authority. ... All VI productions will be cleared for public release **upon completion** except when restricted by security classification, production, or when the production contains copyrighted material.”
- Paragraph 7-10b(4)k, AR 25-1: “The local [PAO] ... will review all unclassified imagery for **possible public release** unless otherwise directed by Office of the Chief, Public Affairs, or higher authority. All multimedia / VI productions will be reviewed for public exhibition by the PAO **prior to** distribution. VI products produced by the Army (whether in-house or by contract) and cleared for public exhibition become part of the public domain.”
- Paragraph 7-10b(4)k(1), AR 25-1: “Public clearance must be granted for any VI product (such as still or motion media productions, stock footage, or electronic images) **prior to** release to the public or placement on a Website.”

A Web Content Review Program is a method to cope, then, with all the review requirements (we might have missed some references, but you get the idea) – primarily pre-dissemination but also post-dissemination (the quarterly screening requirement). TRADOC’s comprehensive Web Content Review Program includes disparate functions and organizations; considers all assigned roles IAW DoD Web policy; and provides a system whereby those reviews mandated by law and policy may be accomplished before PAO approves release of the information into a public forum. IAW AR 25-2, the **OPSEC and PAO reviews are the minimum mandated pre-dissemination reviews**, but the TRADOC Web Content Review Program offers a “best practice” that can be adapted for local use. And since CIO / G-6 policy and guidance doesn’t always clearly outline that PAO must be one of the reviewers (because of the Public Affairs profession’s role as the primary public-information release authority²⁷), PAOs should be proactive in insisting on being both a pre-dissemination reviewer (IAW AR 25-2 et al) and a post-dissemination reviewer (IAW AR 25-1 et al).

There is another critical “triad” within the TRADOC Web Content Review Program: the content provider, content reviewer, and content manager / Website coordinator. This triad not only serves to safeguard information, as the triad of OPSEC, G-6, and PAO does – the provider / reviewer / manager triad ensures that Web content is accurate, relevant, and timely. Like with the OPSEC / G-6 / PAO triad, the provider / reviewer / manager triad also fulfills DoD and Army mandates, and PAO fits into this triad in all three roles of provider, reviewer, and manager.

“One of the biggest problems we face in improving government Websites is that many agencies still view their Website as an IT project rather than as a core business function. ... Agencies should be required to appoint an editor-in-chief for every Website they maintain. ... This person should be given appropriate funding and authority to develop and enforce Web policies and publishing standards, including ensuring that prime real estate on government Websites is dedicated to helping people find the information they need. ... The U.S. economy loses millions of hours of ‘citizen productivity’ every year when people can’t efficiently accomplish basic government tasks on-line, such as filling out a form, applying for a loan, or checking eligibility for a government program. This adds to people’s dissatisfaction with their government.” – **Putting Citizens First: Transforming On-line Government**, Federal Web Managers Council whitepaper

The content-review process and the roles within it are discussed in the next section and in subsequent chapters of this *Guide*. Each of these roles is vital to the successful execution of any Web Content Review Program.

ROLES: CONTENT PROVIDER, CONTENT REVIEWER, CONTENT MANAGER

Content providers. As stated, organizational heads must establish clearance-review procedures for official DoD information that his / her Web-content provider prepares and proposes to post to the organization’s publicly accessible Website. That review process actually starts with the content provider (see Chapter 2), who should be as trained and knowledgeable about the review process as the content reviewers and organizational Website coordinator / command Web-content manager. Content providers should, for instance, be familiar with the rules governing FOUO information. Content providers should also be familiar with the aspects of the organization’s operations considered critical. The content provider should also take into account the form in which the information is to be distributed – such as press releases, press conferences, or publicly disseminated documents on the Web – the susceptibility of the information to data-mining, and the likelihood that the information could directly lead to the discovery and presentment of knowledge that is otherwise controlled (for example, classified information or FOUO information). The content provider shares this latter responsibility with the organizational OPSEC officer. Also to be assessed is a specific risk to the Army’s credibility if publicly released information is omitted and / or deleted from the Web – this is determined by the command PAO, in conference with the content provider and Website coordinator.

²⁷ For an example of this authority, see Paragraph 2-3b(2), AR 380-10, which states that the proponent for disclosure of U.S. Army public-domain information is Public Affairs. Also, Paragraph 2-4m in the new AR 360-1 is expected to specify that PAOs, Army command (ACOM) level and below, are their commander’s designated review and approval authority for the release of official information to the public.

The organization's content providers, content reviewers, and Website coordinators determine whether the information is public or non-public as a first step.

Content reviewers. As illustrated previously in this chapter, a Web Content Review Program is mandated. Who is expected to participate and what they review is covered in more detail in Chapter 3. In short, content reviewers in a robust Web Content Review Program are OPSEC, security (G-2), QI, Staff Judge Advocate (SJA), and PAO professionals. Both the TRADOC G-6 and TRADOC PAO have mandated roles and responsibilities for TRADOC's publicly accessible Web content and share overall monitoring responsibilities.²⁸

Every Army employee is an ad hoc content reviewer, as everyone serves as a "first line of defense" in keeping information off the Internet that could endanger Soldiers' lives and / or affect mission accomplishment. DoD and Army regulations and guidance make each person individually responsible for safeguarding information.²⁹

TRADOC mirrors DoD and Army Web-management structure in that TRADOC PAO acts in concert with the Deputy Chief of Staff (DCS), G-6, to provide oversight and control of content on TRADOC public Websites.³⁰ However, other TRADOC agencies have mandated responsibilities for Web content, such as for OPSEC,³¹ security,³² and information-quality reviews.³³ The SJA advises on copyright, conflict-of-interest, and endorsement issues. All serve as members of the overall TRADOC Web Content Team, as do content providers and leaders. As discussed previously, content-team members help make sure that information of force-protection concern, as well as information not complying with policy / guidance, is not disseminated on the publicly accessible Web. Content-team members also help ensure that their organizations adopt robust QI oversight.

"Many Websites tout organizational achievements instead of effectively delivering basic information and services. ... Many Web managers don't have access to social-media tools because of legal, security, privacy, and internal policy concerns. Many agencies focus more on technology and Website infrastructure than improving content and service delivery. Technology should not drive our business decisions, but rather help us serve the needs of the American people." – **Putting Citizens First: Transforming On-line Government**, Federal Web Managers Council whitepaper

²⁸ AR 25-1, DA PAM 25-1-1, and TR 25-1 describe G-6 functions. (Especially see Paragraph 5-5, TR 25-1, for Webmaster and portal administrator functions and responsibilities.) These regulations also describe Public Affairs' functions, but other regulations and memoranda include PAO responsibilities: e.g., DoDD 5122.5, DoDI 5400.13, AR 530-1, AR 360-1, AR 25-1, AR 25-2, OCPA memorandum "Required Public Affairs Review of Information Released Publicly via Army Headquarters Websites" dated April 28, 2003, and the TRADOC OPSEC Plan. In essence, these references, in conjunction with the ones cited on Pages 13-14, **require Public Affairs' involvement in publicly accessible Web content – both its review and management.**

²⁹ For example, see ALDODACT message 11/06; Paragraph 4-20g(7), AR 25-2; Paragraph 2-1, AR 530-1; Paragraph 1-9, AR 380-5; Paragraph 5-4a, AR 360-1; Paragraph 6a(9), TRADOC OPSEC Plan; OSD memo, "Withholding of Personally Identifying Information Under the Freedom of Information Act (FOIA)," Nov. 9, 2001; ALARACT message 138/2006, "DoD Personnel Responsibility for Safeguarding Personally Identifiable Information," May 26, 2006; and Paragraph 5-5c(1), TR 25-1.

³⁰ Paragraph 2-9b, AR 25-1; and expected as Paragraphs 2-2c(15) and (16), new AR 360-1. This is carried over from DoD Web policy (see Paragraphs 5.1 and 5.1.2, Part I), which requires the DoD CIO and ASD-PA to coordinate on providing policy oversight and guidance to ensure the "effective dissemination" of defense information via the Internet. "Effective dissemination" includes what is not disseminated as well as what is.

³¹ OPSEC review prior to dissemination is required by DoDD 5205.2, AR 530-1, AR 360-1, AR 25-2, the TRADOC OPSEC Plan, and TR 25-1, as well as guidance from the SECDEF ("Website OPSEC Discrepancies," Jan. 14, 2003; also released as ALDODACT 02/03) and a joint message from the DEPSECDEF / VCJCS (ALDODACT message 11/06, "Information Security / Website Alert," Aug. 9, 2006).

³² Security reviews, which are related but not the same as OPSEC reviews (see Paragraph 3, Enclosure A, of CJCSI 3213.01B, and Paragraphs 1-6b and G-1 of AR 530-1 for contrasts between OPSEC and security), are required when information is "intended for public release that pertains to military matters, national security issues, or subjects of significant concern to [DoD]," IAW DoDD 5230.9, DoDI 5230.29, and ALDODACT message 11/06.

³³ Information quality is a federal law (Section 515 of Public Law 106-554; H.R. 5658; Treasury and General Government Appropriations Act for Fiscal Year 2001, or the Information Quality Law) and is outlined in the DEPSECDEF memorandum, "Ensuring Quality of Information Disseminated to the Public by the Department of Defense," Feb. 10, 2003, and HQ DA Letter 25-03-02, "Ensuring Quality of Information Disseminated to the Public by the Department of Defense," Oct. 28, 2003. The Army's QI standards are also discussed in Paragraph 7-7 of DA PAM 25-1-1.

Other important content-team members at HQ TRADOC are the working groups: the WCWG, OPSEC Working Group (OWG), and Webmaster Working Group (WWG). Each working group focuses on different aspects of the TRADOC Web Content Review Program. The WCWG works with Public Affairs; the WWG with G-6; and the OWG with the TRADOC OPSEC officer. QI is a benchmark for all the working groups.

Website coordinators and Web-content managers. Another essential team member is the Website coordinator or Web-content manager. The Website coordinator is a non-Public Affairs professional appointed at organizational level when the organization is co-located with its HQ – such as at a major subordinate organization (MSO) like Army Capabilities Integration Center (ARCIC) or a DCS office co-located with HQ TRADOC – or, at CoE, a school within the command – like the Engineer School within the Maneuver Support Center (MANSCEN). The Web-content manager is a Public Affairs professional appointed at the HQ of an ACOM, MSO such as the U.S. Army Combined Arms Center (USACAC), or CoE.³⁴ The Web-content manager exercises ACOM-, MSO-, or CoE-wide responsibility. The Web-content manager should be the “editor-in-chief” advocated by the Federal Web Managers Council – more on this in Chapter 4.

All HQ TRADOC organizations should have a Website coordinator appointed to assist his / her organization’s workforce in producing and managing the organization’s Web-based products, and to coordinate design (as needed) and clearance of those products with TRADOC PAO. The Website coordinator should serve as a consultant throughout the Web-product development process, providing guidance and maintaining communication between his / her organization and TRADOC PAO. More specific duties and responsibilities for the Website coordinator are outlined in Chapter 4.

Important subgroups (target audiences) for Web products in most commands are first-term Soldiers, junior noncommissioned officers (NCOs), senior NCOs, company-grade officers, field-grade officers, spouses, children, and civilian employees. In many commands there are also Reserve Officer Training Corps (ROTC) cadets, Reserve Component Soldiers, retirees, and local nationals who have their own special information needs.

The Web-content manager at HQ TRADOC is TRADOC PAO. As part of those responsibilities, TRADOC PAO reviews and releases all content intended for the public WWW and AKO’s unrestricted-content areas. Other Web-content manager responsibilities are:

- Maintains HQ TRADOC-level content and monitors the maintenance of deputy commanding general (DCG)- and DCS-level content;
- Manages TRADOC’s Web marketing and outreach efforts;
- In conjunction with the TRADOC Strategic Communication Cell, researches and develops long-term and annual strategies, goals, and objectives for TRADOC Web products;
- In coordination with G-6, develops and organizes content while promoting a consistent look and feel on all HQ TRADOC Web products;
- Establishes procedures and standards for Web products;
- In conjunction with G-6, recommends and interprets federal, DoD, DA, and TRADOC Web-content policies; and
- Provides direction, guidance, and training for content providers, content reviewers, and Website coordinators via telephone, email, or the WCWG and WCWG portal.

Since AR 25-1 uses the terms “Web manager” and “Web maintainer” as synonyms for “Webmaster” – which is not what we mean here at all – a quick digression is in order on how CIO / G-6 Web management differs from PAO Web management, although this will be discussed more in Chapter 4.

CIO / G-6 maintains technical control (techcon)³⁵ of Websites, and provides overall policy and procedural guidance, plus format conventions, regarding the establishment, operation, and maintenance of Army public Websites and

³⁴ Installation PAOs supporting TRADOC senior commanders are considered Web-content managers in TRADOC, IAW Paragraph 1-5i(2), TR 25-1. If the draft of the new AR 360-1 remains unchanged at publication, this will also be true IAW Paragraph 2-4n, which states that PAOs ACOM level and below are their command’s Web-content manager.

³⁵ Paragraph 6-7a(13)(c), AR 25-1.

services.³⁶ CIO / G-6 manages Webservers and other networks. In other words, CIO / G-6 Web management heavily emphasizes the means of delivery of the content, and the format the content appears in. TRADOC G-6's roles are outlined in some detail in TR 25-1, but in essence the G-6 serves as the TRADOC Internet / Intranet administrator (Webmaster) and, overall, is responsible for planning and directing the TRADOC WWW presence, including promulgating TRADOC Web policies. G-6 also reviews Web content for compliance to policy, security risks, and design deficiencies. G-6 chairs the TRADOC WWG and serves on the TRADOC WCWG and OWG.

On the other hand, PAO Web management is specific to content, including relationships with the public and strategies for communicating with that public via Army public Websites. PAO Web-content management also helps ensure relevant, quality information that adheres to the QI law. The Web not only allows an Army commander to reach a wider audience,³⁷ but to better serve most, if not all, the subgroups in his / her command.³⁸ Each subgroup has some unique information needs that can be met with well-planned Web products. (The 18-24 year-olds, especially, relate better to social media and Web products than, say, print or broadcast products.) PAOs assist in formulating and releasing command messages³⁹ that are relevant to those subgroups; supervise the preparation, production, and distribution of Public Affairs Web information⁴⁰; and develop Web materials and products to meet the command's special Public Affairs needs.⁴¹

Just as Public Affairs is an inherently governmental function requiring that official command spokespersons be military or DoD / Army civilian employees, the function of communicating with both the public and internal audiences is inherently a Public Affairs function. Public Affairs professionals are official command spokespersons, designated by the commander and responsible for releasing information pertaining to their command.⁴² (In fact, paralleling DoDD 5122.5, Public Affairs is the sole release authority for official DoD information.) As command spokespersons, PAOs provide unclassified information about the Army and its activities to the public with maximum disclosure and minimum delay,⁴³ and release unfavorable news with the same care and speed as favorable news.⁴⁴ PAOs are charged to be candid with the American people⁴⁵ and ensure that all information provided to internal or external audiences is accurate.⁴⁶

As previously stated, the Web is a powerful means of providing information to the public. Robust PAO Web-content management can ensure that the command's and subordinate organizations' Webpages are treated as a core business function and therefore focus on providing accurate, value-added information services and Web products to organization users, customers, the Army, and the public by sharing relevant information. As a core business function, TRADOC Webpages should also enhance execution of the command's mission by saving resources currently expended on traditional means of communication (e.g., print and broadcast), to ensure all organizations fully leverage the WWW's capabilities in a manner that is efficient and resource-wise.

Content-review subjects are covered in more detail in Chapter 3, but there are two areas of special emphasis for PAOs as Web-content managers: assessing information that needs to be protected, and avoiding endorsement.

PAOs must identify and not release information that would adversely affect national security, threaten the personal safety, or invade the privacy of members of the armed forces⁴⁷ – and they must balance this against the FOIA. PAOs must ensure that their own Web products, and other products generated at their commands, meet OPSEC requirements.⁴⁸ And, of course, PAOs must protect information classified in the interest of national security under AR 380-5.⁴⁹

³⁶ Paragraph 5.1.1, Part I, DoD Web policy; Paragraphs 6-7a(1) and 6-7c(1), AR 25-1; ALARACT "Website Security Policy Compliance," Dec. 19, 2008.

³⁷ Paragraph 5-6c(4), AR 360-1.

³⁸ Paragraph 5-6c(6), AR 360-1.

³⁹ Paragraph 2-4b, AR 360-1.

⁴⁰ Paragraph 2-4e, AR 360-1.

⁴¹ Paragraph 2-4k, AR 360-1.

⁴² See Paragraph 2-3a(2), AR 360-1.

⁴³ Paragraph 2-3d(5), AR 360-1.

⁴⁴ Paragraph 2-3d(6), AR 360-1.

⁴⁵ Ibid.

⁴⁶ Paragraph 2-3d(7), AR 360-1.

⁴⁷ Paragraph 2-3d(5), AR 360-1.

⁴⁸ Paragraph 5-6c(4), AR 360-1.

⁴⁹ Paragraph 2-3d(10), AR 360-1.

Another area that Web-content managers should keep a weather eye on is endorsement or “selective benefit” – and **information that is left out can imply endorsement as much as information that is present**. The Army must not selectively benefit, or appear to benefit, any person, group or corporation, whether profit or non-profit; religion, sect, religious or sectarian sub-group, or quasi-religious or ideological movement; fraternal organization; political organization; or commercial venture. Treatment of non-federal entities must be even-handed; **Army commands or organizations that provide support to non-federal entities must be willing to provide equal support – including via Web content and links – to comparable non-federal entities**. And, of course, Public Affairs must do likewise; PAO is prohibited from supporting any event involving, or appearing to involve, the promotion, endorsement, or sponsorship of any individual, civilian enterprise, religious or sectarian movement, organization, ideological movement, or political campaign.⁵⁰

A prime example of where robust Web-content management could have benefited a command was the situation of Protestant Bible study guides posted by the post chaplain’s office on its Website. Deemed anti-Semitic, the study guides were removed from the command Website after the Military Religious Freedom Foundation, a nonprofit watchdog group that “encourages” the military to enforce separation of church and state, threatened a lawsuit. The foundation said that the “subjective” Bible study guides shouldn’t have been allowed to be posted to a government Website, according to an article by the *Kansas City Star* published June 14, 2007. The study guides were written by a lay leader in the mid-1980s and had apparently been available on the chaplain’s Website for at least five years.

The Army lessons-learned perspective is that the study guides were subjective and did not meet the “no selective benefit” standards. Posting the study guides, without posting like materials from other Christian denominations, or even other religions, made it seem like the command was endorsing the religious viewpoint contained in the study guides to the exclusion of other viewpoints. Therefore the command appeared to selectively benefit, via the presence of the material on its official Website, a religion (Christianity) and, further, a religious group (Protestantism) – and Public Affairs’ management of the command’s Web content made it seem like PAO was endorsing a religion and a religious sect.

Vigilance in analyzing the repercussions of both absent and present content is a major responsibility of the Web-content manager.

⁵⁰ Paragraphs 3-2a and b(1), AR 360-1.

Chapter 2

The content provider

As stated in Chapter 1, posting content to public Websites incurs a responsibility for the information provider. This chapter explores the role and expectations of the Web-content provider in more detail.

THE CONTENT PROVIDER'S ROLE IN THE ORGANIZATIONAL WEBSITE

The Webmaster does much of the work involved in the organizational Website's development and design, but the content provider has an important role. Good design attracts visitors the first time; good content keeps them coming back. Good design includes planning good content. And good content is obligatory, as TRADOC's public Website is a vital tool for communicating with the public, the rest of the Army, the media, and other important communities. TRADOC's "public face" offers a perfect opportunity to share information, lessons-learned, and topics of concern. It's important for content providers to recognize that the TRADOC public Website represents a critical viewpoint on the command: a first impression by an American taxpayer, a resource for a congressional staffer, an on-line library for U.S. allies, or a "reassurance" that TRADOC is developing the Army's future leaders well. It's important that our visitors' experience with our Websites be a positive one.

Good design is what your visitor sees first and what makes the content accessible to him or her. But good design is nothing if your content is dull, outdated, or nonexistent. Content must be relevant, interesting, unique, accessible, and current. Therefore the content provider's role in the success of the organization's Website – to create good content – cannot be underestimated.

WRITING FOR THE WEB: IT'S A STRATEGY

To create good content, know the "10 Commandments for content providers":

- **Know the purpose of the organizational Website and the purpose of the Webpage.** Refer to the Website's purpose statement and plan (see Chapter 4) with everything you write so that you include in the Website content *only* the information that supports the Website's purpose – nothing peripheral. Ensure that the purpose of the Webpage is clear and unambiguous. What's the purpose of the page? State it in the first paragraph. What does the audience want to know about the subject? What do you need to tell them? Content must be relevant to the Website's topics and visitor's information needs.
- **Know the organization's goals for the Website.** Make a list of these goals, something the Website strives for, and make sure the Website content does its part in meeting the organization's goals. If the site doesn't have goals itself, you won't know whether it's working for you. What should the audience do after they read the Webpage? Make sure it's obvious – what are the next steps?
- **Know your target audience**, what matters to them, what they're interested in, and tailor the content. Content needs to offer Website visitors what they need and want. Who is your intended audience? What do they want to know? What do you need to tell them? Does your content anticipate their obvious questions? Did you lead them to related materials?
- **Be mindful of and support the Website's budget in time and money.** A Website's budget is the amount of time and / or money the content provider, content reviewer, Web-content manager, and Webmaster can spend on it. It's safe to assume that available time to work on the Website is limited.

For example, if you want to use an imagemap as part of your Webpage's content, ensure that your imagemap is carefully designed and its use carefully considered. Imagemaps heighten a Webpage's visual impact but can be time-consuming to maintain, since when the coordinate structure changes, Webmasters must update the coordinates in both the image and the map files. To help save time, Webmasters should use client-side instead of server-side imagemaps except where the area cannot be defined by an available geometric shape.

- **Understand technological and Website-visitor limitations.** Technological limitations include connections – e.g., not making a Webpage graphics-heavy if visitors come to the Website via dialup – and the size of the visitor's monitor. If most visitors' monitors are small, for instance, think in terms of screens, not pages, and write content in short blocks. The content provider must also consider the human limitations. Less than 10 percent of your first-time visitors will scroll beyond the top of your Webpage, so the top four inches of your page are crucial. Content must make its point and portray its relevance to the visitor in those four inches. This is a point that content providers must work on closely with the Web designer so that the top four inches aren't completely taken up by banners / logos and navigation elements. Content must be written and organized

efficiently – people don’t like to read on the screen, so keep it short and sweet. Seventy-nine percent of Web users scan, so use about 50 percent of the words you’d use in print publishing. A rule-of-thumb is to limit a Webpage to two printed pages long if possible, or provide target tags to various sections of the document to assist readers in finding content. (See “content must be accessible,” below.)

In case the Website visitor comes to the Website via dialup, graphics creators / editors should set graphics at a resolution of no more than 72 dots per inch (dpi). (However, keep in mind that graphics created at lower resolutions than 72 dpi have less chance of meeting QI standards.) Scanned images should also be set at 72 dpi. Graphics creators / editors should reduce the number of colors in their color palette whenever possible.

“We have too much content to categorize, search, and manage effectively, and there is no comprehensive system for removing or archiving old or underused content. Some agencies have posted competing Websites on similar topics, creating duplication of effort and causing confusion for the public. Much government Web content is written in ‘governmentese’ instead of plain language.” – **Putting Citizens First: Transforming On-line Government**, Federal Web Managers Council whitepaper

- Closely related to the preceding “commandment” is that **content must be interesting**. To make content interesting, include illustrations or charts. Break up large blocks of text into more manageable paragraphs and include art. Write as if you were talking to someone face-to-face – use a conversational tone and don’t use Army jargon or clichés. To make keywords stand out, use highlighting (bold print). Highlight only key information-carrying words; avoid highlighting entire sentences or long phrases. Remember that bulleted and numbered lists can draw attention to important points.
- **Content must be unique**, not available elsewhere. Of course your site should provide links to other relevant sites, but it’s your site’s unique content that will draw people back to it. Avoid duplication and redundancy. (And by all means, make sure content doesn’t contradict other information on the site.)
- **Content must be accessible** – not in the sense of Section 508-compliant here, but easily reached and searched. (Section 508 compliance is detailed in Appendix N.) Create *internal links*, showing clear links to the main sections in your site and label those links so it’s obvious what they contain. If your text mentions items of interest, hyperlink your visitors by way of words, phrases, or subheads. Create *external links* also – if

information already exists on another Website about the same subject or about subjects referenced on your Webpage, link to that information. If you anticipate that your visitors will want to know something that’s beyond your scope, take them where they can find what they’re looking for through links. When you link to other sites, practice “deep linking” – work with your Webmaster to not merely link to the homepage and leave visitors to their own devices, but link directly to the information you want your site visitor to see. Good, deep links leave visitors with a favorable impression of you and will bring visitors back to your site. People should be able to easily reach the useful information in your site. External links should add value and / or relate to your Website. The words for the links should describe the link – no “click here” links. Ensure the Webmaster has established a *search function* and that you work with him / her to provide suggested metatags⁵¹ and keywords to aid site searchability.

- **The content must be current**. Update your content frequently, deleting outdated information and adding new information. Provide the most current information available, with no dead or outdated external links. Visitors who encounter links that don’t work and/or stale or wrong content most of the time don’t return to those sites again.
- **Check your spelling, punctuation, and syntax** (grammar, sentence structure, and language rules). Spelling and punctuation must be accurate. Always proofread text before posting it on-line, even after others have reviewed it for content. Spelling mistakes or typing errors are unprofessional and embarrassing, while factual errors or misleading information can damage the reputation of both the content provider and the organization.⁵²

⁵¹ See Paragraph 8-3b(9), DA PAM 25-1-1, for the Army’s metadata / metatag requirements, which must be included on all homepages and major entry points. See Paragraph 5-3c, TR 25-1, for TRADOC’s metatag requirements.

⁵² This paragraph should be a baseline QI standard, part of every organization’s QI program.

If you must use acronyms, use them only after you've spelled them out once. Present information using plain language that considers the knowledge and literacy level of the typical Website visitor.⁵³ The text must be gender-neutral and accessible to persons who, as a result of national origin, are limited in their English proficiency.

Understandable language and content criteria should be included in the organization's annual customer-satisfaction survey.⁵⁴

See Appendix M for more tips on writing for the Web.

WRITING FOR THE WEB: STYLE

It's also a writing strategy, although not an obvious one, to use a conversational and consistent style. (Inconsistency is jarring to the reader.) Army journalism style is conversational and should be the style used. This section outlines the style a content provider should use, as well as common mistakes with words and usage.

Use the *Associated Press Stylebook and Briefing on Media Law* as the preferred style guide, and *Webster's New World Dictionary of the American Language*, Second College Edition (or equivalent) as the preferred dictionary.⁵⁵

Following are guidelines for some of the more frequently encountered aspects of Web-content style:

- **Acronyms** – Spell out on first reference.
- **Capitalization** –
 - Don't capitalize names of things unless the thing is unique, but capitalize the names of major DoD, DA, or TRADOC programs if they're the only ones of their kind.
 - Capitalize a person's title if it is used before his / her name; do not capitalize a title if used as an appositive (set off by commas) after a person's name. Don't capitalize *commander* or *commanding general* – these should not be used before names, but only as appositives after names.
 - Don't capitalize words that refer to capitalized words but are used as standalone words, such as *command* when referring to TRADOC or *department* when referring to DoD.
 - *Soldier* must be capitalized when referring to U.S. Soldiers.⁵⁶
- **Dates and times** should use the following guidelines:
 - Use civilian form of dates (e.g., March 13, 2008, not 13 Mar 08).
 - Use numerals without *th*, *st*, *nd*, or *rd* (e.g., Nov. 23 not Nov. 23rd).
 - Spell out the name of the month when using it with a year but without a day (e.g., November 2008).
 - When using a specific date, abbreviate the month. Do not abbreviate March, April, May, June, or July.
 - Do not use the year unless it is not the current year.
 - Use lowercase for a.m. and p.m., and use periods.
 - Use an en dash with no spaces if time spans or dates are inclusive (e.g., 8-11 a.m. not 8 a.m. to 11 a.m.).
 - Use an en dash with no space if dates are inclusive (e.g., May 12-22 not May 12 to 22).
- **Dimensions** – Use figures and spell out *inches*, *feet*, *yards*, etc., to indicate depth, height, length, and width. Hyphenate adjectival forms before nouns. Use an apostrophe to indicate feet and quote marks to indicate inches (e.g., 5'6") only in very technical contexts. Examples:
 - He is 5 feet 6 inches tall.
 - The 5-foot-6-inch man
 - The 5-foot man

⁵³ This is a federal standard; refer to the "federal requirements" section of Chapter 4 (Page 135).

⁵⁴ Paragraph 8-3b(3), DA PAM 25-1-1.

⁵⁵ Paragraph 13-12a, AR 360-1.

⁵⁶ By order of Chief of Staff, Army (CSA). This will become written policy for command information (CI) products – for example, expected as Paragraph 13-12b(4) when the new AR 360-1 is published.

The basketball team signed a 7-footer.
The car is 17 feet long, 6 feet wide and 5 feet high.
The rug is 9 feet by 12 feet.
The 9-by-12 rug
The storm left 5 inches of snow.

- **Name** – Use only the last name in subsequent reference regardless of gender.⁵⁷
- **Numbers** should use the following guidelines:
 - Spell out a number if it is the first word in a sentence.
 - Spell out numbers below 10. Use numerals for 10 and above.
 - Use numerals exclusively in dimensions, ratios, proportions, military units, and dates.
- **Phone and fax numbers** should be written as follows: (555) 555-5555; DSN 555-5555. Commercial toll-free numbers with DSN equivalents should be listed as (xxx) xxx-xxxx, DSN (zzz) zzz-zzzz.
- **Punctuation** – Do not use a comma before the conjunction in a series (e.g., Tom, Dick and Harry). Do use a comma to close an appositive (further identifies or adds background information on a person, place, or thing) or separate any other independent clause from the rest of the sentence (e.g., *Col. Tom Martin, commander of the 555th Training Brigade, said* – “commander of the 555th Training Brigade” is the appositive and is both preceded and closed by a comma).
- **Rank** –
 - Refer to Soldiers by rank rather than by pay grade (for example, E-6 or O-5). Refer to pay grade only in pay scales.⁵⁸
 - Omit a Soldier’s rank in sports and other competition stories.⁵⁹
 - When using an Army rank before a name, use these rank abbreviations:

Rank	Usage before a name
general	Gen.
lieutenant general	Lt. Gen.
major general	Maj. Gen.
brigadier general	Brig. Gen.
colonel	Col.
lieutenant colonel	Lt. Col.
major	Maj.
captain	Capt.
first lieutenant	1st Lt.
second lieutenant	2nd Lt.
chief warrant officer 5	CW5
chief warrant officer 4	CW4
chief warrant officer 3	CW3
chief warrant officer 2	CW2
warrant officer 1	WO1
command sergeant major	Command Sgt. Maj.
sergeant major	Sgt. Maj.
first sergeant	1st Sgt.
master sergeant	Master Sgt.
sergeant first class	Sgt. 1st Class
staff sergeant	Staff Sgt.
sergeant	Sgt.
corporal	Cpl.
specialist	Spc.
private first class	Pfc.

⁵⁷ Paragraph 13-12b(1), AR 360-1.

⁵⁸ Paragraph 13-12b(2), AR 360-1.

⁵⁹ Paragraph 13-12b(3), AR 360-1.

private

Pvt.

Common mistakes with word usage include:

- **Affect, effect** – *Affect*, as a verb, means *to influence*. *Affect* as a noun is best avoided; it's occasionally used in psychology but not in everyday language. *Effect*, as a verb, means *to cause*. *Effect* as a noun means *result*.
- **Compose, comprise, constitute** – *Compose* means *to create or put together*. It's commonly used in both active and passive voices. *Comprise* means *to contain, to include all or embrace*. Use only in active voice. *Constitute*, in the sense of *form* or *makeup*, is used if neither *compose* nor *comprise* fit.
- **Email, e-mail** – Use *email*, without the hyphen and no capitalization, unless it begins a sentence or is in a headline.
- **Ensure, insure** – Use *ensure* to mean *guarantee*. (Example: Steps were taken to ensure accuracy.) Use *insure* only for references to insurance. (Example: The policy insures his life.)
- **Include** – Use when what follows is part of the total. Do not use *etc.* at the sentence's end. Example: *My job includes sizing photographs for the magazine layout.* Not: *My job includes sizing photographs, etc.*
- **More than, over** – *Over* is a physical position. When dealing with numbers, use *more than* – such as *more than 90 percent* (not *over 90 percent*).
- **Online, on-line** – Use *on-line*.
- **Set up, setup and log on, logon** – Use *set up* and *log on* as verbs in instructions (e.g., *set up the printer* or *log on the network*.) *Setup* and *logon* are adjectives or nouns (e.g., *the setup program* or *your logon password*.) This rule goes for other similar pairs like *back up* and *backup*.
- **Who, that, which** – When a phrase or clause refers to an animal with a name or to a human being, introduce the phrase / clause with *who* or *whom*. (Do not use commas if the clause is essential to the sentence's meaning; use them if it isn't.) *That* is the preferred pronoun to introduce clauses that refer to an inanimate object or an animal without a name. *Which* is the only acceptable pronoun to introduce a non-essential clause that refers to an inanimate object or an animal without a name. *Which* may occasionally be substituted for *that* in introducing an essential clause that refers to an inanimate object or an animal without a name. In general, this use of *which* should appear only when *that* is used as a conjunction to introduce another clause in the same sentence: *He said Monday that the part of the Army which suffered severe casualties needs reinforcement.* Follow this rule even if your word-processor's spelling and grammar check function prompts you to change your use of *who*, *that* or *which* in your writing.
- **WWW, www and Web, web** – Use *the Web* or *WWW* in text and *www* in Uniform Resource Locators (URLs). If you're being formal, spell out *Worldwide Web* using initial capital letters. If you're writing about aspects of the Web, use *Webpage* or *Website*. (In spite of how the regulations use *Webpage*, *Website*, *Webserver* and like words, they are words portraying one idea and thus *Web* should not be spaced from the rest of the word.)

CONTENT PROVIDERS AND THE REVIEW PROCESS

Once the content provider has prepared quality content, the next step is to staff the content through the review process before it is posted (called *pre-dissemination review*). Content providers should know the requirements before sending content through the review process.

Following are the requirements, functions, and expectations of organizational Web-content providers (denoted by the symbol ❖, with explanatory notes included).

- ❖ Content providers are expected to coordinate review of Web content through all steps (more information on the steps of the review process is contained in the next chapter). For content the provider is responsible for, coordinate for the OPSEC review,⁶⁰ security review if needed, SJA review if needed, and QI review before submitting content to TRADOC PAO. Content providers serve as the organization's responsible party to

⁶⁰ Paragraph 5-4, AR 360-1.

the organization's leadership⁶¹ for the content. Content intended for posting to AKO / Defense Knowledge On-line (DKO) unrestricted-content areas must also be cleared by all reviewers.⁶²

Minor content changes (aka "pen-and-ink" changes such as those that once would have been done in pen on printed pages – for Web-content purposes, these are slight changes that do not significantly affect the meaning or nuance of the content, such as email or phone number updates, or change in date when an event is rescheduled) to existing content on the Web **do not require advance approval** from TRADOC PAO or other approval authorities.

- ❖ **Content providers are expected to help the organization make an initial determination on whether the level of accessibility for the Web content will be public or limited** (non-public).⁶³ As part of this determination, the content provider takes into account the form in which the information will be distributed, the susceptibility of the information to data-mining, and the likelihood the information could directly lead to the discovery and dissemination of knowledge that is otherwise controlled (e.g., classified information or FOUO information).⁶⁴ Provide input to Public Affairs on the risk to the organization's credibility if publicly released information is omitted and / or deleted from the Web.

Content providers should be involved in determining whether information is public or private as a first step because there are review and posting procedures for AKO / DKO as well as for the publicly accessible Web, IAW AR 25-1. Not only must organizations establish procedures (e.g., a review process) for content providers to place information on AKO / DKO – same as the general-public Web – but also, AKO / DKO content and the organization's posting procedures must conform to DoD and Army Website policy. (Therefore **posting to AKO / DKO isn't an "escape" from the review process mandated for the publicly accessible Web – AKO / DKO has much the same process unless the content will be posted to an area that has a positive access control** – for more on access controls, see Chapter 4.) Organizations must also ensure that organizational Webmasters (Web administrators) assign security and access controls that content providers request – it is part of the Webmaster's job to set up mechanisms to protect sensitive information from access by unauthorized individuals.⁶⁵ **In short, whether the content is headed for the public or non-public side, there's some kind of review process.**

Of note: **there may be instances when PAO will review / clear content to be published on a non-public server. Three general rules-of-thumb are:**

- Content to be published to controlled-access Websites doesn't require PAO review / approval but does require OPSEC review. This doesn't include the unrestricted-content areas of AKO / DKO, which **do** require PAO review / approval – see below.
- However, content that offers formal presentation of an official TRADOC position / message destined for publication on **any** Website – whether unclassified, controlled-access, or classified – must be reviewed / approved by PAO.
- If content is to be posted to AKO / DKO as "unrestricted content" – that is, made available to all AKO / DKO users and groups – it must be treated as publicly accessible content and must be reviewed by PAO.⁶⁶
- ❖ **Content providers must do their part to help ensure the quality, objectivity, utility, and integrity of organizational information disseminated to the general public.** Focus on providing value-added information to the organization's users, customers, the Army, and the public through accurate, timely, and relevant information.⁶⁷ Ensure information is accurate and adheres to published DoD and Army policies.⁶⁸
- ❖ **Content providers should keep records of reviews,** IAW Paragraph 7-7j of DA Pamphlet (DA PAM) 25-1-1, Chapter 8 of AR 25-1, Paragraphs 1-13 and 4-15b of AR 380-5, and OMB memorandum M-05-04, "Policies for Federal Agency Public Websites," Dec. 17, 2004. (See Chapter 4 for a breakdown of the

⁶¹ Paragraph E-9, AR 380-5.

⁶² Paragraph 6-7d(4), AR 25-1; Paragraph 2-3a(15), AR 530-1.

⁶³ Paragraph 5-3b, TR 25-1.

⁶⁴ Paragraph 3.5.2.2, Part II, DoD Web policy.

⁶⁵ Paragraph 6-7d(4), AR 25-1.

⁶⁶ Paragraph 6-7d(4), AR 25-1. See also Paragraphs 6-7d(5) and 6-7d(7), AR 25-1: "All AKO / DKO account users are responsible for the security of ... content they create on the portal. Users [who] fail to properly secure their AKO / DKO credentials and content on the AKO / DKO portal will be subject to non-judicial or judicial action under the Uniform Code of Military Justice (UCMJ)."

⁶⁷ Memorandum from DISC4, "Guidance for Management of Publicly Accessible U.S. Army Websites," Nov. 30, 1998.

⁶⁸ Paragraph 5-4b, AR 360-1.

federal requirements for Websites.) Content providers must manage Web records per OMB Circular A-130 and guidance from the National Archives and Records Administration (NARA) (see 36 CFR 1220-1238 and www.archives.gov/records_management/index.html).

- ❖ Website content providers and administrators will **support and participate in feedback reporting**. (See Appendix O.)

When content providers submit materials for pre-dissemination review / approval, they may use the checklist at the end of this chapter to improve the coordination and review process. (See Chapter 3 for a breakdown of this process.) PAOs supporting TRADOC CoE commanders / senior commanders⁶⁹ may adapt the checklist for local use.

GENERAL MILITARY REQUIREMENTS

Beyond knowing what specific actions he / she should take within his / her organization regarding Web-content review, **the content provider should also have an overall idea of what the requirements are for military Websites**, since he / she will be directly or peripherally involved with those requirements. In general, DoD and Army policy require each Website / Webpage or publicly accessible portal page⁷⁰ to:

- Have a verified valid mission need to disseminate the information;⁷¹
- Go through proper management and TRADOC content-review procedures;⁷²
- Comply with DoD Website administration policy, Army Website policy (AR 25-1), Army information-resource management policy (DA PAM 25-1-1), TRADOC regulations, and guidance for official, publicly accessible Websites, and any subsequent policies and guidance memorandums;
- Be reviewed for OPSEC and security according to current OPSEC methodology.⁷³ Information must be protected according to its sensitivity, and details must be limited to what is necessary;
- Be Section 508 compliant IAW Section 1194.22 of the 508 standards;⁷⁴
- Be reviewed and released by Public Affairs, as all information contained on publicly accessible Websites is public information – even if intended for an internal audience – and is therefore subject to the policies and clearance procedures prescribed in Chapter 5, AR 360-1, for release of information to the public;⁷⁵
- Be reviewed every quarter for accuracy and timeliness of content;
- Be implemented in such a way as to support the widest range of potential users and computing platforms;
- Use any of the Hypertext Markup Language (HTML) specifications recommended by the Worldwide Web Consortium (W3C);⁷⁶ and

⁶⁹ Usage of the term “senior commander” as defined by the new version of AR 600-20 (rapid-action revision dated Feb. 11, 2009, to regulation dated March 18, 2008) here assumes that one individual is dual-hatted as both the senior commander and the TRADOC senior mission commander. The “senior commander” is normally the senior general officer on an installation and is designated by senior Army leadership (CSA and SecArmy), and thus derives his / her command authority over the installation by direct delegation from the CSA and SecArmy. The senior commander is also the “senior mission commander” where that title is mentioned in Army regulations (except for regulations involving operational duties and responsibilities – mission commanders retain those duties and responsibilities). The senior commander’s responsibilities and authorities are installation-focused, while the mission commander’s responsibilities and authorities are mission-focused – thus the dual hat. This **Guide** adds the adjective “TRADOC” in front of “senior commander” for specificity, in case the senior commander (who is also the installation commander) is not the senior leader on the installation and thus is not dual-hatted as both senior commander and senior mission commander – the senior commander could possibly be the senior leader of another tenant on the installation, for example. This **Guide** only addresses TRADOC entities and the organizations that support TRADOC entities. The TRADOC senior commander’s PAO, as used in this **Guide**, is the PAO responsible for supporting TRADOC’s senior leader on the installation. For more information on the senior commander, mission commander, installation commander, and garrison commander roles, see Paragraph 2-5b, AR 600-20.

⁷⁰ Not access-controlled beyond basic AKO authentication. See Chapter 3.

⁷¹ SECDEF message, “Website OPSEC Discrepancies,” Jan. 14, 2003; Paragraph 5b(5)(a), TRADOC OPSEC Plan.

⁷² SECDEF message, “Website OPSEC Discrepancies,” Jan. 14, 2003.

⁷³ SECDEF message, “Website OPSEC Discrepancies,” Jan. 14, 2003; Paragraph 3-3i, AR 25-2; Paragraphs 5b(5)(b) and 6a(9), TRADOC OPSEC Plan. See also Paragraph 4.3.1, DoDD 5205.02.

⁷⁴ Paragraph 6-7a(14), AR 25-1.

⁷⁵ Paragraph 6-7c(3), AR 25-1; Paragraph 13-14, AR 360-1.

- Be an official Army Website and be located on the army.mil domain – which is required of all Army public and non-public Websites unless the CIO / G-6 waives the requirement.⁷⁷

GRAPHICS / IMAGES / MULTIMEDIA GUIDELINES

Images (e.g., graphic arts and photography) and multimedia / VI are Web content and have their own usage requirements, outlined following. **Official DoD imagery provided on publicly accessible TRADOC Websites must both conform to DoDD 5040.5⁷⁸ and be reviewed for OPSEC,** just like text. Use of images on the Web must also consider the content's usability for Website visitors. (See Section 508 requirements, Appendix N).

As mentioned, images and multimedia undergo the review process as well. Images and multimedia should be considered in the QI review process. Multimedia / VI must be validated by the functional proponent and cleared for public release before being placed on a Website for viewing or downloading.⁷⁹ The procedures in the next chapter and Appendix K can assist in the clearance process.

Following are general guidelines for using photographs and video on the WWW. Non-compliance to any of them can put a “stopper” in obtaining permission to post content.

Altering DoD imagery. Although content providers will want to customize imagery for their own Websites, it is DoD and Army policy that alteration of official DoD / Army imagery “by persons acting for or on behalf of” DoD / the Army is prohibited. However, the following modifications are authorized:⁸⁰

- Photographic techniques common to traditional darkrooms and digital imaging stations (such as dodging, burning, color balancing, spotting, and contrast adjustment) that are used to accurately record an event or object are not considered alterations.
- Photographic and video image techniques for enhancing, exploiting, and simulating unique cartography; topography; engineering; geodesy; intelligence; criminal investigation; medical; research, development, test, and evaluation (RDT&E); scientific; and training requirements are authorized if they do not misrepresent the subject of the original image.
- Obviously masking portions of a photographic image for specific security, criminal-investigation, privacy, or legal requirements is authorized.
- Cropping, editing, or enlarging to selectively isolate, link, or display a portion of a photographic or video image is not considered alteration. Cropping, editing, or image enlargement that misrepresents the facts or circumstances of the event or object as originally recorded constitutes a prohibited alteration.
- Digitally converting and compressing photographic and video imagery is authorized.
- Photographic and video post-production enhancements (including animation, digital simulation, graphics, and special effects) used for dramatic or narrative effect in education, recruiting, safety, and training illustrations, publications, or productions is authorized under either of the following conditions:
 - The enhancement does not misrepresent the subject of the original image; and
 - It is clearly and readily apparent from the context of the image or accompanying text that the enhanced image is not intended to be an accurate representation of any actual event.⁸¹

⁷⁶ Addressed by AR 25-1 and the DoD Web policy. Although not “set in stone” by DoD or Army policy, DoD and the Army do consider the W3C reliable. For instance, in Paragraph 4-14c(1), AR 25-1, data-standards producers are required to use W3C technical specifications holding a “recommended” status to ensure maximum operability. (A W3C recommendation is a technical report that is the end result of extensive consensus building about a particular technology or policy.) Further, Section 508 requirements in AR 25-1 are based on W3C recommendations. In Paragraph 10.1, Part II, of the DoD Web policy, DoD requires Website documents to conform to the approved technical specifications approved in the Joint Technical Architecture (JTA), but where W3C’s work is more recent than the JTA’s, Web developers may use W3C recommendations or proposed recommendations. Usage of W3C recommendations regarding HTML specifications ensures the widest range of utility for the general public, including accessibility under Section 508.

⁷⁷ Paragraph 6-7a(5), AR 25-1.

⁷⁸ Paragraph 8, Part II, DoD Web policy.

⁷⁹ Paragraph 7-7a(6)(b)19, AR 25-1.

⁸⁰ Paragraph 4.4, DoDI 5040.5; Paragraph 13-4c, AR 360-1. See also Paragraph 7-7b(1)(b), AR 25-1: “The alteration of official imagery by any means for any purposes other than to establish the image as the most accurate reproduction of a person, event, or object is prohibited.”

⁸¹ Paragraph 7-7b(1)(c), AR 25-1.

Photograph quality. Photographs on the Web must support Public Affairs' goals, objectives, and principles. All photographs should be of the highest photojournalistic quality. This means photographic reporting that visually communicates information with a journalistic view of the subject or event.⁸²

Photos help bring your Web content to life. Ask a photographer to take photos for you. If you're doing the shooting, follow these tips to help obtain journalistic quality:

- Fill the camera frame with the subject. Get in close.
- Avoid putting too many people in one shot, and make sure the subject is in focus.
- Watch for objects in the background; they may be distracting. If someone looks like he / she has a flagpole growing out of his / her head when you're looking at him / her in your camera's viewfinder, try to move him / her to one side or the other.
- Try to shoot pictures that have people moving into the center of the photo, not out of it.
- The best photos are those that show action. Avoid "grip-and-grins," where one person hands something to another one while shaking hands, and both stare at the camera. Get the subject doing his or her job.
- If you can't avoid a grip-and-grin, such as photographing an award presentation, at least try to get the presenter and presentee close together. They won't be comfortable standing close, but try and move them so they're almost head to head and both looking at the award. Otherwise, there will be "lotsa wall" – a gap that will look huge in the resulting photograph. Again, it's best to get the subject doing his or her job and avoid this altogether. This is what will look more eye-catching to the Website visitor.
- Remember to gather complete information for the photo's outline. A photo outline identifies the people, equipment, or other subjects of the photo. The outline should have the five Ws (who, what, when, where, and why – see Appendix M, writing for the Web) in them. The outline should also describe the action and provide background information.

Public Affairs photography support. Official photography, television, audio, and graphic-art support to public-information programs such as Army Websites is authorized, but recording and reproducing must be limited to the minimum required to satisfy official needs⁸³ – there should be no gratuitous graphics that add Webpage "weight" without content value. For most of these events, the content provider must request support from the local Directorate of Information Management (DOIM)'s training-support center. Materials and requirements for products, services, and capabilities meeting criteria for VI record documentation (e.g., promotion boards, ceremonies, changes of command, or social events that aren't newsworthy) must be processed according to AR 25-1. Requests to alter VI products must also go to the local DOIM.⁸⁴

It's inappropriate to request a Public Affairs photographer for events that would be record documentation, as Public Affairs is authorized to take news-related photographs only.⁸⁵ For VIP visits, Public Affairs coverage would be restricted to photography and video that would meet the minimum essential requirements.⁸⁶

Copyrighted material. Recording, duplicating, and / or using copyrighted material in the development of any VI production is prohibited by law (Title 17 U.S. Code (USC), copyrights) unless prior permission from the copyright owner is obtained in writing.⁸⁷ (Evidence of this consent must also be maintained throughout the lifecycle of the product.) If a person obtains written permission, his / her use, duplication, and electronic alteration of commercially obtained electronic images must be IAW applicable copyrights and licenses.⁸⁸ Content providers should consult the SJA for guidance.

Content providers should not assume they can use pieces of copyrighted material as "fair use" – fair use rarely applies to the military departments, so written permission **must** be obtained. Ownership or possession of copyrighted material does not constitute permission to use or duplicate. The Army holds everyone responsible for preventing copyright infringement; violators are subject to prosecution at all levels of involvement.⁸⁹

⁸² Paragraph 13-4b, AR 360-1.

⁸³ Paragraph 5-8, AR 360-1.

⁸⁴ Paragraph 3-7, AR 360-1.

⁸⁵ Paragraph 5-8d, AR 360-1.

⁸⁶ Paragraph 5-8b, AR 360-1.

⁸⁷ Paragraphs 7-7a(4) and 7-11d, AR 25-1. Also see Paragraph 7-12d, AR 25-1.

⁸⁸ Paragraph 7-7b(1)(d), AR 25-1.

⁸⁹ Paragraph 7-11d, AR 25-1.

Organizationally sponsored videos. Army multimedia / VI productions may not be used to promote organizations and commands; promote sales of commercial products or private industries; influence pending legislation; or provide forums for opinions on broad subjects. (See DoDD 5040.3). Multimedia / VI-production content may not be incompatible or inconsistent with Army policies / doctrine; discriminate against or stereotype individuals on the basis of gender, race, disability, creed, nationality, age, religion, national origin, or sexual orientation; or weaken / cast doubt on the Army's or DoD's credibility.⁹⁰

Prohibited recordings and photographs. There are **some items that are prohibited from photo-optical and electronic recording** (Title 18 USC, Chapter 25),⁹¹ so content providers should not provide these items for requested Web content, since offenders are subject to fines and punishment:

- Photographs of money – genuine or counterfeit, foreign or domestic, or any portion thereof;
 - However, photographs of money are authorized in black-and-white for philatelic, numismatic, educational, or historical purposes; for publicity in connection with sales and campaigns for U.S. bonds; or for other newsworthy purposes (excludes advertising purposes) provided that such photographs are less than three-quarters or more than 1 ½ the size (in linear dimension) of the money photographed.
 - The negatives (original recording material) and plates used must be destroyed after final use.
 - The term “money” here refers to notes, drafts, bonds, certificates, uncanceled stamps, and monetary securities in any form (31 CFR, Subtitle B, Chapter IV).
- Government transportation requests;
- Passport and immigration or citizenship documents;
- A badge or identification card prescribed by agencies of the U.S. government for use by an officer or employee (18 USC 701);
- Selective Service registration card;
- Foreign government, bank, or corporation obligations; and
- Property titles when regulated, restricted, or prohibited by the issuing state.

PAO AS CONTENT PROVIDER

Public Affairs is, or should be, a major Web-content provider. From the Public Affairs perspective, part of the public is our own CI target audience. Whatever emphasis is given to releasing information to the external media, the same (or greater) emphasis should be given to our internal media – which includes not only CI newspapers and broadcast facilities, but also Army Websites; the Web is a CI and public-communications tool rolled into one. The Web, in fact, is an extraordinarily important Public Affairs tool due to its public access and its immediate information-release capability. However, **the Web is often overlooked as a Public Affairs tool**.

Commanders and their PAOs can use the Web to tell the Army story and correct disinformation / distortions as quickly as possible. In fact, a SECDEF / Chairman of the Joint Chiefs of Staff (CJCS) message issued to combatant commanders regarding support of Public Affairs activities in potential future military operations charged commanders to “approach these decisions [on Public Affairs support and releasing information] with ‘why not’ rather than ‘why’? ... The goal for moving both media products and images should be minutes or hours, not days.”

There are several responsibilities, roles, and expectations unique to Public Affairs as content providers to the public, especially for Web content. Public Affairs is the commander's principal adviser for newsmedia relations, public liaison, internal communications, community relations, audiovisual matters, and Public Affairs and VI training.⁹² In this capacity, Public Affairs is:

- The **sole release authority** to newsmedia representatives for official DoD information and audiovisual materials, as defined by DoDD 5230.09 – including, but not limited to, press releases. PAO is responsible for ensuring a free flow of general and military news and information – without censorship or propaganda – to the newsmedia, general public, DoD's internal audiences (e.g., the men and women of the armed forces and their family members; civilian employees; contractors who work for DoD), and other applicable

⁹⁰ Paragraph 7-11b, AR 25-1.

⁹¹ Paragraph 7-11c, AR 25-1.

⁹² Paragraph 3 and Enclosure 2, DoDD 5122.05.

forums, limited only by the security restraints in DoDD 5200.1 and any other applicable statutory mandates or exemptions.

- The principal spokesperson for the command. The PAO is the office responsible for formulating and releasing command messages. The PAO may designate additional spokespersons as required.
- The official point-of-contact (POC) for the commanding general (CG)'s and DCG's public and media activities. The PAO is responsible for developing short- and long-range plans to communicate leaders' policies and major programs – and to support execution of these plans, including advance programming and event coordination with other government agencies and with private, public, and media organizations.
- The official POC for public release of the CG's or DCG's speeches, public statements, congressional testimony, articles for publication, and other materials. As an Army obligation to the public, the sole purpose of providing information about what leaders think, say, or write is to expedite the flow of information about Army leaders' policies to the public – propaganda and self-aggrandizement have no place in Public Affairs operations.
- The official POC to receive, analyze, and reply to the general public's inquiries on command policies, programs, activities, news trends, and media coverage. PAO coordinates, prepares, and provides to the referring office, as required, media-coverage analysis, data, and breaking news in reply to public inquiries. Information about the command's policies must be disseminated impartially and objectively.
- The responsible office to prepare, produce, and distribute printed and electronic (Website) Public Affairs information. As mentioned in Chapter 1, Public Affairs develops materials and products to meet the command's special Public Affairs needs.

At installation level, Public Affairs is charged to develop, acquire, and / or produce timely news and information programming, distributed through installation broadcast facilities. The command Website should provide information on command-channel programming and post-newspaper coverage, linking the major news-and-information distribution venues.

Public Affairs is also responsible for:⁹³

- Watching over and ensuring that information is not classified or otherwise withheld to protect the government from criticism or embarrassment; and
- Ensuring that requests for information from organizations and private citizens are answered in a timely manner.

To manage all these responsibilities, Public Affairs needs to proactively employ the Web and manage content. (See Chapter 4.)

⁹³ Paragraph 3 and Enclosure 2, DoDD 5122.05.

TRADOC Pre-Dissemination Content Review Procedures Checklist

Subject of email submitting materials for review: "For content review [subject to be reviewed]."

Send to TRADOC PAO's content-review email address, monr.contentreview@monroe.army.mil, or to TRADOC PAO's generic email address, tradocpao@monroe.army.mil. (TRADOC senior commanders' PAOs should provide a generic local email address for their supported personnel to contact or to submit material for review.)

Name and contact information of content provider (email and direct-line telephone number):

Department / organization submitting content to be reviewed:

Name of page author(s), if different from content provider:

Target date for information to be posted:

Determined to need password protection?	Yes []	No []
If so, meets guidance for effective password protection?	Yes []	No []
PKI-enabled?	Yes []	No []
FOUO document?	Yes [] (May not be posted to the public Web without formal OPSEC risk assessment; alternate means of posting should be explored.)	No []
Is page Section 508 compliant?	Yes [] (Provide organizational Webmaster's verification summary / results generation.)	No [] (Provide justification on why document does not have to meet Section 508 compliance. If justification not provided or waiver of Section 508 compliance not granted, page must be brought into compliance before being posted.)
Has content been reviewed for OPSEC?	Yes [] (Provide copy of organizational OPSEC reviewer's assessment.)	No [] (Must be accomplished before submission to PAO.)
Has content been reviewed for classified information, IAW DoDI 5230.29?	Yes [] (Provide security reviewer's assessment or statement that none of the content is classified or classified by compilation.)	No []
Has content been reviewed for Quality of Information (QI)?	Yes [] (Provide summary of what QI review(s) have been performed.)	No [] (Accomplish before submission to PAO.)

Has content been reviewed by legal counsel?	Yes [] (Provide summary of opinion, including name and contact information, or statement from counsel that there are no legal issues in this content.)	No []
Will content need clearance higher than TRADOC, such as by OSR (Paragraph 6.1, DoDI 5230.29) or OSD (Paragraph 5-3, AR 360-1)? (See Appendix K.)	Yes [] (Explain and provide recommendation on releasability.)	No []
Summary of content:		
Website URL (intended or planned):		
Check one: New page [] Revision [] Major change [] (List and describe in the "Comments" section).		
List of specific files / documents to be reviewed (list separately):		
Information for Webmaster – list of planned metatags: My keywords are: My description is:		
Comments:		

The "keywords" metatag should convey the subject matter of the Webpage or resource. Keywords should be expressed as words or phrases that describe the theme or content of the page or resource. Try to imagine the terms someone outside your area would use in a search engine to find information on your Webpages.

The "description" metatag should contain a brief textual description of the content of the Webpage or resource. This may include abstracts or summaries, or content descriptions. Use complete sentences and good grammar; some search engines will use this summary in your displayed search results.

Chapter 3

Content reviewers / the content review

This chapter is a continuously building narrative like the first two chapters, but it is also designed to “take apart” and use in sections – for instance, the OPSEC reviewer could concentrate on the OPSEC-review section to the exclusion of most of the rest of the chapter. The chapter primarily spells out what each type of reviewer, as named in Chapter 1, is responsible for reviewing.

In essence, it is the content reviewer’s job to screen for non-public, non-releasable information as defined by the stipulations and principles in Chapter 1. To identify non-public information, check to see if the information is (if it is, it shouldn’t be posted):

- Personally identifiable and subject to the Privacy Act;
- Classified according to the National Security Act;
- Subject to a FOIA exemption; or
- Otherwise “sensitive.”

PERSONALLY IDENTIFIABLE AND SUBJECT TO THE PRIVACY ACT

The Privacy Act of 1974 (5 USC 552a), implemented by AR 340-21, prohibits any Army member from publicly releasing PII – which is defined as any information that can be used to identify an individual⁹⁴ – without prior written consent by that individual.⁹⁵ The Army’s Privacy Act Program provides a comprehensive framework regulating how DA collects, maintains, uses, or disseminates personal information on individuals; the program provides balance between DA’s information requirements and the individual’s privacy interests and concerns.⁹⁶ DoD Public Affairs organizations are required to comply with the requirements of DoDD 5400.11 (the DoD privacy program) when their actions involve releasing PII.⁹⁷

Some key provisions of the Privacy Act / AR 340-21:

- The act covers living citizens of the United States and aliens lawfully admitted for permanent residence – it does not, however, confer any privacy rights on the dead.⁹⁸
- The Privacy Act requires federal agencies to establish proper administrative, technical, and physical safeguards to ensure the security and confidentiality of records, and to protect against any threats or hazards to an individual’s security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness. (Also see OMB document M-07-16.)⁹⁹
- Managers of *systems of records*¹⁰⁰ must ensure that all personnel – including government contractors or their employees who design, develop, operate, maintain, or control any system of records – are informed of all requirements to protect the privacy of the individual whom the record concerns.¹⁰¹

⁹⁴ Definitions section, Part III, DoD Web policy. See also the glossary of AR 340-21, where “personal information” – AR 340-21 does not use the term “personally identifiable information” – is defined as “[i]nformation about an individual that is intimate or private to the individual, as distinguished from information related solely to the individual’s official functions or public life.”

⁹⁵ Paragraph 5-15, AR 360-1; Paragraph 1-5, AR 340-21. Paragraph 3-1, AR 340-21; Appendix R, FM 3-61.1; Chapter 5, AR 360-1; and Appendix K, AR 360-1, list what is releasable on persons under the Privacy Act. Also see ALARACT message 138/2006, “DoD Personnel Responsibility for Safeguarding Personally Identifiable Information,” May 26, 2006: “In general, the statutory and regulatory authority limits the ... dissemination of ... information except with the consent of the individual about whom the information pertains or as otherwise may be authorized by one of the enumerated exceptions to the [Privacy] Act.” Because PII is FOUO (see FOIA section, this chapter), however, the provision of “consent” must be balanced with a formal OPSEC assessment of the risk that releasing PII on the publicly accessible Web incurs; security overrides “consent” and “general Public Affairs considerations,” IAW guidance in the DEPSECDEF’s memo, “Information Vulnerability and the Worldwide Web,” Sept. 24, 1998.

⁹⁶ Paragraph 8-5h, AR 25-1.

⁹⁷ Paragraph 3d, DoDD 5122.05. DoDD 5400.11 consists mostly of policy on disclosure from a system of records (Paragraph 4.6), as does AR 340-21, but does provide the foundational principles for releasing any PII.

⁹⁸ Paragraph 1-5 and glossary, AR 340-21; Paragraph K-1, Appendix K, AR 360-1. Next-of-kin may not exercise any rights for deceased family members. A parent or legal guardian may exercise Privacy Act rights for a minor or an incompetent individual.

⁹⁹ Paragraph 4-4a, AR 340-21.

¹⁰⁰ IAW AR 340-21, a *system of records* is “[a] group of records under the control of DA from which information is retrieved by the individual’s name or by some identifying number, symbol, or other identifying particular assigned to the individual.” A group

- Personal information is usually given at least the protection required for FOUO information. Privacy Act data must be afforded reasonable safeguards to prevent inadvertent or unauthorized disclosure.¹⁰²
- A Soldier or DA employee may be found guilty of a misdemeanor and fined up to \$5,000 for willfully disclosing PII to someone not entitled to it.¹⁰³

The term *system of records* is key in AR 340-21. The conceptual framework of the regulation is that, IAW Paragraph 1-1, it sets policies and procedures governing personal information that DA keeps in systems of records, therefore the reg applies to extraction of information from those systems of records. But there are exceptions for the exceptions. For example, the 12 exceptions¹⁰⁴ to the Privacy Act's "no disclosure without consent" rule permit the release of certain PII without the individual's consent; **one of the exceptions to the Privacy Act's must-have-consent provisions is when the FOIA requires release of the record** – the Privacy Act can't prevent release of information if the FOIA requires release. (See the FOIA section, next page.) *Requires* is a key word, as information must not be discretionarily released under the FOIA if the information is subject to the Privacy Act's "no disclosure without consent" rule.

Obviously, the Privacy Act has an intertwining relationship with the FOIA. A Privacy Act request for access to records must also be processed as a FOIA request. If the requester will be denied access to all or any part of the requested PII, the PII must be considered under the provisions of both the Privacy Act and the FOIA; withholding any information must be justified with a legally applicable exemption in each act.¹⁰⁵

So how do you apply the Privacy Act to decisions regarding release of PII on the Web if that PII isn't from a system of records? It's common-sense, since the principles are the same, to not release PII – putting aside the issue of whether it's from a system of records or not – if it's considered non-releasable by the Privacy Act. Therefore, keeping the Privacy Act's limitations in mind, **content reviewers should screen for sensitive (non-releasable) PII, which includes:**

- **Individual** – A person's age, date of birth, place of birth, Social Security number (SSN), home of record, home address, home telephone number, race / ethnic origin, religious affiliation, citizenship, identity (i.e., name) if the individual is a confidential informant / witness in a law-enforcement investigation;
- **Education** – Educational level, civilian-education degrees and major areas of study, school and year of graduation, college grades;
- **Family** – Marital status, family members' names / sexes / SSNs, legitimacy of children, details of family fights / reputation / ordeals;
- **Health** – Type of leave taken, health / life insurance, medical details / conditions;
- **Jobs / assignments** – Overseas assignments (present or future), office or unit mailing address if at a sensitive station or outside the United States, duty phone of routinely deployable or sensitive units, outside employment, performance ratings / evaluations, proposed reduction-in-force status, union affiliation, almost anything about law-enforcement personnel;
- **Conduct** – Disciplinary actions, existence of investigations, most misconduct (especially lower mid-level employees), criminal history, reason for termination, unsubstantiated allegations / accusations, sexual inclinations and association;
- **Financial** – Financial status, financial statement(s); and
- **Information that would otherwise be protected from mandatory disclosure under a FOIA exemption.**¹⁰⁶

Content reviewers must also screen with an eye on recent guidance that has made what's releasable more restrictive because of risk to DoD personnel – see the FOIA and "special problems of PII" sections later in this chapter. For

or series of files arranged chronologically or subjectively, but not retrieved by individual identifier, is not a system of records, even though a person's information could be retrieved by an individual identifier via document-by-document search.

¹⁰¹ Paragraph 4-8, AR 340-21.

¹⁰² Paragraph 4-4c, AR 340-21.

¹⁰³ Paragraph 4-9b, AR 340-21.

¹⁰⁴ See Paragraph 3-1, AR 340-21, for the 12 exceptions to the Privacy Act, or the privacy briefing at <https://www.rmda.army.mil/privacy/docs/pa1974-overview.mht> on the RMDA Website, Slide 48.

¹⁰⁵ Paragraph 2-3, AR 340-21.

¹⁰⁶ Appendix K, AR 360-1; privacy briefing at <https://www.rmda.army.mil/privacy/docs/pa1974-overview.mht> on the RMDA Website, especially Slides 8 and 9.

instance, the Office of the SECDEF's (OSD) policy memorandum of October 2001 (see Footnote 133), provided greater protection of DoD personnel in the aftermath of the terrorist attacks Sept. 11, 2001. OSD's memo requires information that personally identifies DoD personnel to be carefully scrutinized and limited. In general, DoD requires that its components not release lists of names, duty addresses, present or past position titles, grades, salaries, and performance standards of DoD military members and civilian employees.¹⁰⁷ On posted memoranda such as command policy letters and delegations of authority, point-of-contact (POC) contact information listed in the memo may include name, official title, organization, and office telephone number. No other information, including room numbers, is to be included about these POCs. On the other hand, there are some items of PII that may not be withheld – see the FOIA section later in this chapter.

The “special problems of PII” section later in this chapter discusses, in some detail, the ins and outs of releasing PII. Additionally, a checklist at the end of this chapter outlines what information, including PII, is definitely releasable, what is conditionally releasable, and what isn't releasable according to Army regulations. Appendix J has a consolidated list of PII according to recent guidance. Content reviewers should consider the policy and principles contained in these tools in making their determination whether to clear content for release or not.

CLASSIFIED ACCORDING TO THE NATIONAL SECURITY ACT

The Army's information-security (INFOSEC) program, implementing the National Security Act via AR 380-5, applies to information 1) that requires protection to prevent damage to national security and 2) has been classified IAW Executive Order (EO) 12958 or its predecessors. AR 380-5 delineates the Army's policy for classifying, downgrading, declassifying, transmitting, transporting, and safeguarding information requiring protection in the interests of national security. The regulation primarily pertains to classified information but also addresses controlled unclassified information (CUI), including FOUO and “sensitive but unclassified” (SBU).

Classified information also comes under Exemption 1 of the FOIA. (See the next section in this chapter.)

DoDD 5230.9 and DoDI 5230.29 require a security and policy review to be performed on “all official DoD information intended for public release that pertains to military matters, national-security issues, or subjects of significant concern to [DoD].”¹⁰⁸ In many cases, information that pertains to national-security issues may be classified. See the definitions section in this *Guide* for more details on what “national security information” is.

Classified information, of course, is prohibited from release on a publicly accessible Website.¹⁰⁹

SUBJECT TO A FOIA EXEMPTION

The FOIA is an information-disclosure federal statute that uses an exemption structure, discussed in the next paragraph, to strike a balance between the competing interests of information disclosure and nondisclosure, with emphasis on *fullest responsible disclosure*.¹¹⁰ The FOIA's “core purpose” is to “shed light on an agency's performance of its statutory duties,”¹¹¹ so disclosure should focus on information that supports how an agency fulfills its duties. The Army's FOIA program implements DoD's FOIA policy requiring DoD activities to conduct business in an open manner and to provide the public a maximum amount of accurate and timely information concerning its activities, consistent with the legitimate public and private interests of the American people.¹¹²

¹⁰⁷ Section 505.7, 32 CFR, *The Army Privacy Program*.

¹⁰⁸ Paragraph 4, DoDI 5230.29. Also see Paragraph 5-1, AR 360-1.

¹⁰⁹ Paragraph 6-7c(4)(b), AR 25-1. Not only is release of classified information a FOIA exemption and under the jurisdiction of AR 380-5, but network-security policy also pertains. IAW Paragraphs 4-16b, 4-16g, and 4-20c(1), AR 25-2, transmission and storage of classified content (which would involve a Webserver and the Webserver's “calling” of documents) must be done on secure systems, not on publicly accessible ones: “All Army personnel and contractors will mark, ship, store, process, and transmit classified or sensitive information [IAW] AR 380-5”; “All Army personnel and contractors will not transmit classified information over any communication system unless using approved security procedures and practices, including encryption, secure networks, secure workstations, and ISS accredited at the appropriate classification level”; and “Supervisors and managers will [e]nsure transmission of classified or sensitive information via applicable secure means.” AKO-SIPRNET can be used for classified content, according to Paragraph 4, ALARACT 089/2008.

¹¹⁰ Department of Justice (DoJ)'s *Freedom of Information Act Guide*, 2007, http://www.usdoj.gov/oip/foia_guide07.htm. DoJ also has comprehensive information on its FOIA Website, <http://www.usdoj.gov/oip/index.html>, including case-law applications and principles.

¹¹¹ From the Supreme Court's 1989 landmark FOIA decision in *United States Department of Justice v. Reporters Committee for Freedom of the Press*, cited in the DoJ's FOIA guide, http://www.usdoj.gov/oip/foia_guide07.htm.

¹¹² Paragraph 8-5g, AR 25-1.

The FOIA, in essence, provides that any person has a right, enforceable in court, to obtain access to federal records – except to the extent that these records, or parts of them, are protected from public disclosure by one of nine statutory exemptions.¹¹³ The FOIA’s exemption categories protect against disclosure of information that would harm national defense or foreign policy, privacy of individuals, proprietary interests of business, the function of government, etc.¹¹⁴ For example, the exemption concerning PII is the personal-privacy exemption (Exemption 6), which provides that personnel, medical, and “similar files,” which constitute a clearly unwarranted invasion of personal privacy, are FOIA-exempt.¹¹⁵ (We’ll come back to Exemption 6 later in this section.)

CUI as described in AR 380-5 includes FOUO information as an overlapping category, but *FOUO* derives its meaning from the FOIA: FOUO is specifically defined as unclassified information which is exempt from mandatory release to the public under the FOIA.¹¹⁶ (By definition, information must be unclassified to be designated FOUO. Therefore if information fits into one of the FOIA-exempt categories – except Exemption 1, classified information – the information is FOUO.) Therefore **content reviewers must be familiar with the FOIA exemptions in determining whether content is FOUO**. Content reviewers should also be alert to the significant changes that the Open Government Act of 2007 and the upcoming Open Government Directive (to be issued by OMB)¹¹⁷ have made / will make to the FOIA.

¹¹³ Joint memo from the director of the Army Staff and the administrative assistant to the SecArmy, “Freedom of Information Act (FOIA) Program,” Sept. 17, 2008.

¹¹⁴ Although federal agencies may make “discretionary disclosures” of exempt information when they’re not specifically prohibited from doing so, agencies are constrained from making discretionary disclosures for certain exemptions. This footnote provides a synopsis of the exemptions and notes the nondiscretionary-exemption categories, but see Chapter III, AR 25-55, for details. The types of information covered by FOIA exemptions are:

- 1) **Exemption 1, classified documents** – these protect national defense or foreign policy. Includes classification by compilation. As discussed in the previous section of this chapter, this exemption is **nondiscretionary** – this information may not be released.
- 2) **Exemption 2, internal personnel rules and practices** – involves matters related solely to an agency’s internal personnel rules and practices. This category is **discretionary**. There are two separate classes in this category: trivial administrative matters of no genuine public interest and internal manuals whose disclosure would risk circumvention of law or agency regulations.
- 3) **Exemption 3, information exempt under other laws** – covers other laws that restrict availability of information, such as the provision in the tax code that prohibits public disclosure of tax returns and tax-return information. **Nondiscretionary** category. There are some 48 applications of this exemption; in addition to prohibiting the release of tax-return information, other prohibitions include grand-jury information, census data, information about the National Security Agency (NSA), financial and media records, and national historic preservation, for example.
- 4) **Exemption 4, confidential business information** – protects trade secrets and proprietary information from disclosure. Also exempt: privileged or confidential commercial or financial information obtained from a person. For the most part, Exemption 4 protects information about private commercial interests and is a **nondiscretionary** FOIA-disclosure category. Specifically, the Trade Secrets Act, a criminal statute, prohibits the unauthorized disclosure of most, if not all, the information falling within Exemption 4.
- 5) **Exemption 5, internal government communications** – intra-agency and interagency memorandums or letters are exempt from disclosure. This is to safeguard the “deliberations” inherent in the policy-making process of government. For example, correspondence between government departments regarding joint decisions does not have to be disclosed. However, this is a **discretionary** category.
- 6) **Exemption 6, personal privacy** – personnel, medical and “similar files,” which constitute a clearly unwarranted invasion of personal privacy, are FOIA exempt. This is a **nondiscretionary** category; however, a balancing of public-interest considerations is built into the determination of whether the information is exempt in the first place. Personal information may also fall into the protective coverage of the Privacy Act, discussed in an earlier section of this chapter.
- 7) **Exemption 7, law enforcement** – allows law-enforcement agencies to withhold records to protect the law-enforcement process from interference. **Discretionary** category, per DoJ. There are six specific sub-exemptions that protect: an active investigation from interference, individuals from being denied a fair trial, against the unwarranted invasion of personal privacy, the identity of confidential sources, information that would reveal TTP or guidelines for law-enforcement investigations or prosecutions, and information that could endanger an individual’s life or physical safety.
- 8) **Exemption 8, financial institutions** – this exemption protects information contained in or related to examination, operating or condition reports prepared by or for a bank supervisory agency such as the Federal Deposit Insurance Corporation (FDIC), Federal Reserve or similar agencies. **Discretionary** category.
- 9) **Exemption 9, geological information** – covers geological and geophysical information, data, and maps about wells. **Discretionary** category.

¹¹⁵ Paragraph 1-5a, AR 340-21, includes a similar requirement to protect the privacy of individuals from “unwarranted intrusion,” as required by the Privacy Act.

¹¹⁶ Paragraphs 5-2a and 5-2b, AR 380-5.

¹¹⁷ “Transparency and Open Government” presidential memo, Jan. 21, 2009, http://www.whitehouse.gov/the_press_office/Transparency_and_Open_Government, and FOIA presidential memo, Jan. 21,

In fact, twin memos issued by the President Jan. 21, 2009, on the FOIA and governmental transparency, both which supplement the Open Government Act of 2007, are instructive: “A democracy requires accountability, and accountability requires transparency. ... In our democracy, the [FOIA], which encourages accountability through transparency, is the most prominent expression of a profound national commitment to ensuring an open government. ... The [FOIA] should be administered with a clear presumption: in the face of doubt, openness prevails. The government should not keep information confidential merely ... because of speculative or abstract fears. ... All agencies should adopt a presumption in favor of disclosure ... to renew their commitment to the principles embodied in the FOIA and to usher in a new era of open government. ... The presumption of disclosure also means that agencies should take affirmative steps to make information public. They should not wait for specific requests from the public. All agencies should use modern technology to inform citizens about what is known and done by their government. Disclosure should be timely.”

A follow-up memo issued by the Attorney General March 19, 2009, on the FOIA, reiterated these principles and said: “[A]n agency should not withhold information simply because it may do so legally. I strongly encourage agencies to make discretionary disclosures of information. An agency should not withhold records merely because it can demonstrate, as a technical matter, that the records fall within the scope of a FOIA exemption. [W]henver an agency determines that it cannot make full disclosure of a requested record, it must consider whether it can make partial disclosure. Agencies should always be mindful that the FOIA requires them to take reasonable steps to segregate and release nonexempt information.”¹¹⁸

DA is more restricted in its discretionary release, as much of the information listed in AR 25-1 as prohibited on Army publicly accessible Websites is FOIA-exempt information¹¹⁹ – and information not authorized for a publicly accessible Website is also not releasable in any other public forum.¹²⁰ Per AR 25-1, **Army organizations using the Internet will *not* post the following types of information on the Army’s public Websites:**

- FOIA-exempt – aka FOUO – information¹²¹ (for a more extensive list of FOUO, see Appendix G);
- Records related solely to internal personnel rules and practices that are not meant for public release (Exemption 2 of the FOIA);
- Restricted- or limited-distribution information¹²²;
- Records protected by another law that specifically exempts the information from public release (Exemption 3 of the FOIA). This includes information protected by copyright;
- Trade secrets and commercial or financial information obtained from a private source which would cause substantial competitive harm to the source if disclosed (Exemption 4 of the FOIA)¹²³;
- Internal records that are deliberative in nature and are part of the decision-making process that contain opinions and recommendations (Exemption 5 of the FOIA). This exemption includes draft documents, draft publications, or pre-decisional information of any kind;
- Records which, if released, would result in a clearly unwarranted invasion of personal privacy (Exemption 6 of the FOIA); and
- Investigatory records or information compiled for law-enforcement purposes (Exemption 7 of the FOIA).

Per AR 340-21, **the following category is also prohibited from release under the FOIA:**

- Release of emergency-recall rosters. Emergency recall rosters should only be shared with those who have an “official need to know” the information, and they should be marked FOUO.¹²⁴

2009, http://www.whitehouse.gov/the_press_office/Freedom_of_Information_Act. Also see **FOIA Post** on DoJ Website, <http://www.usdoj.gov/oip/foiapist/2009foiapist8.htm>.

¹¹⁸ Memo available at <http://www.usdoj.gov/ag/foia-memo-march2009.pdf>. Also see **FOIA Post**, <http://www.usdoj.gov/oip/foiapist/2009foiapist5.htm>.

¹¹⁹ Paragraph 6-7c(4), AR 25-1. See Footnote 114 for a synopsis of the FOIA exemptions. Examples of FOUO are given in Paragraphs 3.5.3, Part II, and Paragraphs 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, and 2.7, Part V, DoD Web policy; also Paragraphs 1-5, B-2, Appendix C, and Appendix D, AR 530-1, and Paragraph 5-3b, TR 25-1.

¹²⁰ Paragraph 5-2d(3), AR 530-1.

¹²¹ Also see Paragraphs 1-5, B-2, Appendix C, and Appendix D, AR 530-1.

¹²² Also see Paragraphs 1-5, B-2, Appendix C, and Appendix D, AR 530-1.

¹²³ Also see Paragraph 2.3, Part V, DoD Web policy.

¹²⁴ Section 505.7, 32 CFR, **The Army Privacy Program**.

It has been our experience that PII is one of the most difficult areas to analyze whether to release it or not, and so the next section is devoted to “the special problem of PII.” Here we specifically discuss PII as Exemption 6 of the FOIA. This exemption, as previously stated, permits the federal government to withhold information about individuals contained in personnel and medical files and in “similar files” when disclosure of this information “would constitute a clearly unwarranted invasion of personal privacy.” There are several principles to understand before we go into the problematic area of releasing PII belonging to DoD’s military and civilian employees.

To be protected under Exemption 6, information must first meet what DoJ calls a “threshold requirement”: it must fall within the category of “personnel and medical files and similar files.” “Personnel and medical files” are fairly straightforward, but the meaning of the term “similar files” is more ambiguous, and therefore we must rely on the 1982 Supreme Court decision, in *United States Department of State v. Washington Post Co.*, that Congress intended the term to be interpreted broadly. The court said that protection of an individual’s privacy “surely was not intended to turn upon the label of the file which contains the damaging information” and that **all information that “applies to a particular individual” meets the threshold requirement for Exemption 6 protection**. According to the DoJ, “This means, of course, that this threshold is met if the information applies to any particular, identifiable individual – which makes it readily satisfied in all but the most unusual cases of questionable identifiability.”¹²⁵

Once the threshold requirement is satisfied, the next key principle to consider is whether disclosing the information constitutes a “clearly unwarranted” invasion of personal privacy. Determining this requires balancing the public’s “right to know” against the individual’s right to privacy. First, ascertain whether a “protectable privacy interest” exists that would be threatened by disclosure – if not, the information isn’t protected under Exemption 6. “If a privacy interest is found to exist, the public interest in disclosure, if any, must be weighed against the privacy interest in nondisclosure,” states the DoJ. “If no public interest exists, the information should be protected; as the D.C. Circuit has observed, ‘Something, even a modest privacy interest, outweighs nothing every time.’ Similarly, if the privacy interest outweighs the public interest, the information should be withheld; if the opposite is found to be the case, the information should be released.”¹²⁶

If there is a privacy interest, what will be the harm in disclosure? According to the DoJ, “[a]ny consideration of potential privacy invasions must include both what the requester might do with the information at hand and also what any other requester, or ultimate recipient, might do with it as well. Indeed, it has explicitly been recognized by the D.C. Circuit that ‘[w]here there is a substantial probability that disclosure will cause an interference with personal privacy, it matters not that there may be two or three links in the causal chain.’”¹²⁷

In some cases, disclosure of information may involve no invasion of privacy because no expectation of privacy exists. For example, if the information at issue is particularly well known or is widely available within the public domain, there generally is no expectation of privacy. Nor does an individual have any expectation of privacy with respect to information that he himself has made public.

If determined that a personal-privacy interest is threatened by disclosure, the second step in the balancing process comes into play: assessment of the public’s interest in disclosure. Not a voyeur’s interest, but legitimate public interest in that disclosure involves **personal information that directly reveals the operations or activities of the federal government** – the Supreme Court has repeatedly stressed that information not fitting this definition “falls outside the ambit of the public interest that the FOIA was enacted to serve.” If “public interest” is found under this standard, it must be accorded a measure of value so it can be weighed against the threat to privacy. As the Supreme Court has emphasized, “The public interest sought to be advanced [must be] a significant one.” For example, information that would inform the public of violations of the “public trust” has strong public interest and is given a great deal of weight in the balancing process. As a general rule, demonstrated wrongdoing of a serious and intentional nature by a high-level government official is of enough public interest to outweigh almost any privacy interest of that official.

Once both the privacy interest at stake and the public interest in disclosure have been ascertained, the two competing interests must be weighed against one another. Determine which is the **greater result of disclosure: the harm to personal privacy or the benefit to the public**. “In balancing these interests, the ‘clearly unwarranted’ language of Exemption 6 weights the scales in favor of disclosure, but if the public benefit is weaker than the threat to privacy,

¹²⁵ DoJ FOIA guide, http://www.usdoj.gov/oip/foia_guide07.htm.

¹²⁶ Ibid.

¹²⁷ Ibid.

the latter will prevail and the information should be withheld. The threat to privacy need not be immediate or direct; it need only outweigh the public interest,” according to the DoJ.¹²⁸

Courts regularly uphold the nondisclosure of information concerning marital status; legitimacy of children; welfare payments; family fights and reputation; medical condition; date of birth; religious affiliation; citizenship data; genealogical history establishing membership in a Native American tribe; SSNs; criminal history records; incarceration of U.S. citizens in foreign prisons; sexual inclinations or associations; and financial status. Even “favorable information,” such as details of an employee’s outstanding performance evaluation, can be protected on the basis that it “may well embarrass an individual or incite jealousy” among co-workers. Moreover, release of such information “reveals by omission the identities of employees who did not receive high ratings, creating an invasion of their privacy.”

Some categories of PII are generally not exempt from disclosure under the FOIA and therefore must be released to the public **if requested**. These categories are also not considered sensitive / non-releasable under the Privacy Act. (This doesn’t mean that all the following categories **must** automatically be released on the Web, and indeed, it may not pass OPSEC-sense to do so.) In general, federal civilian employees may have no expectation of privacy regarding their names, titles, grades, salaries, and duty stations, or regarding the parts of their successful employment applications that show their qualifications for their jobs. DoD, historically in most circumstances and as a matter of policy, disclosed the categories of PII shown in the following list for its individual military personnel, as well as comparable information concerning its individual civilian employees. By regulation, DA discloses substantially the same information concerning its military and civilian personnel. However, in light of worldwide terrorism, DoD now regularly withholds PII about all military and civilian employees if disclosure will “raise security or privacy concerns” (and invokes Exemption 6, citing that harm to personal privacy outweighs public benefit), a subject we’ll come back to in the “special problem of PII” section.

If there are no security or privacy concerns, examples of the PII categories that must be released to the public if requested are:

- **Military personnel:** name; rank; date of rank; gross salary; present and past duty assignments; officially established future assignments; office / unit name; duty address and phone number; source of commission; promotion sequence number; awards and decorations; professional military education; civilian-education level if used to qualify for position; non-government position used to qualify for government position; duty status at any given time; separation or retirement dates; military-occupational specialty (MOS); active-duty official attendance at technical, scientific, or professional meetings; and biographies and photos of key personnel. (**Caveat:** Army policy requires withholding of biographies / photos unless the person is a command spokesperson or a general officer (GO) / Senior Executive Service (SES) due to OPSEC concerns, and even then, names of key leaders aggregated across Webpages must be evaluated.)¹²⁹
- **Federal civilian employees:** name; present and past position titles; occupational series and grade; present and past annual-salary rates (including performance awards or bonuses, incentive awards, merit-pay amount, meritorious or distinguished executive ranks, and allowances and differentials); present and past duty stations; non-government position used to qualify for government position; office / duty telephone number; position descriptions; identification of job elements; and performance standards (but not actual performance appraisals). Performance elements and standards (or work expectations) may be withheld when they are so intertwined with performance appraisals that the disclosure would reveal an individual’s performance appraisal.¹³⁰

¹²⁸ DoJ FOIA guide, http://www.usdoj.gov/oip/foia_guide07.htm.

¹²⁹ Paragraph 3-3a(1), AR 340-21; Section 505.7, 32 CFR, *The Army Privacy Program*. However, IAW AR 340-21, lists or compilations of unit / office addresses or telephone numbers of military personnel may not be released when the requester’s main purpose in seeking the information is to use it for commercial solicitation.

¹³⁰ Paragraph 3-3b(1), AR 340-21; Section 505.7, 32 CFR, *The Army Privacy Program*. Disclosure of this information, however, may not be made when the FOIA request is a list of present or past position titles, grades, salaries, and / or duty stations and 1) is selected to constitute a clearly unwarranted invasion of personal privacy (for example, the nature of the request calls for a response that would reveal more about the employee than the items listed above); or 2) would be protected from mandatory disclosure under a FOIA exemption. Also of note, in addition to the information categories listed, this information can be released to a prospective employer of a current or former Army employee: 1) tenure of employment; 2) civil-service status; 3) length of service in the Army and the government; and 4) date and reason for separation shown on the Standard Form 50 (notification of personnel action).

Again, release of this PII must be considered in light of security concerns. PII is protected when personnel are assigned to sensitive, routinely deployable units or stations in foreign territories. Therefore readers who are paying attention realize there could be a mismatch in the following areas between what the Privacy Act says in non-releasable PII and what must be released under the FOIA if requested: military and civilian employees' titles, grades, salaries, duty addresses, and performance standards (see Page 34); civilian-education degrees and level; and present and past assignments, especially if they're overseas. Also, if a Soldier is overseas, just releasing his / her office / unit mailing address is problematic, especially his / her duty phone if he / she is assigned to a routinely deployable or sensitive unit. (See PII section, below.) We recommend that you consult your local FOIA and Privacy Act subject-matter experts (SMEs) in your G-6 for help in knowing whether to recommend release of these PII categories on the publicly accessible Web.

OTHERWISE "SENSITIVE"

Although what is FOIA-exempt can be a slippery slope, "sensitive" information may actually be the hardest category to define. For instance, beyond designation as FOUO, PII may also be considered sensitive information and thus exempt from public disclosure under those provisions; see Paragraph 1-5, AR 530-1.

"Sensitive" is another overlapping category, since it is included in the categories of CUI, but the primary sense used here is AR 530-1's definition: "Information requiring special protection from disclosure that could cause compromise or threat to our national security, an Army organization, activity, family member, DA civilian, or DoD contractor. Sensitive information refers to unclassified information." Appendix I includes examples which may be deemed sensitive as outlined in recent guidance; however, sensitive information is not limited to this list. For instance, examples of sensitive unclassified information given in the SECDEF message, "Website OPSEC Discrepancies," are concepts of operations (CONOPs), operational plans (OPLANs), and standard operating procedures (SOPs).

Other non-releasable information, in addition to FOUO and Privacy-Act-protected information includes these categories of "sensitive" information:

- Casualty information before verification that the Army (or other military service) has formally notified next-of-kin;
- Information regarding incidents under ongoing investigation;
- Information about or imagery of coalition forces without a release signed by the individuals in advance;
- Information about or imagery of enemy personnel killed in action (KIA), wounded in action (WIA), or hospitalized;
- Information that misrepresents the Army;
- Statements in conflict with good order, morale, discipline, and mission accomplishment; or
- Photographs containing sensitive images, especially those showing the results of improvised-explosive-device (IED) strikes, battle scenes, casualties, and destroyed or damaged equipment.

Therefore, while information may not be precisely FOUO (not exempted from disclosure by the FOIA), it might be sensitive and subject to DoDD 5230.9 / DoDI 5230.29's guidance on information intended for public release that pertains to military matters, national-security issues, or subjects of significant concern to DoD.

An OPSEC / security checklist at the end of this chapter should aid content reviewers in making their determination whether to clear content for public release. Appendices E through H contain lists of critical information, CUI, FOUO, and OPSEC indicators, respectively.

THE SPECIAL PROBLEM OF PII

While the Army engages adversaries in what leaders have termed an "era of persistent conflict," PII¹³¹ has been linked with OPSEC and has even been designated as FOUO. Federal, DoD, and Army policy and guidance on PII was continuously issued as the national emergency continued (declared by the President Sept. 14, 2001, and

¹³¹ As defined by OMB document M-07-16, PII is not differentiated between an individual's private and public lives. Per OMB M-07-16, PII is information which can be used to distinguish or trace an individual's identity – such as his / her name, SSN, or biometric records – alone or when combined with other information linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. PII includes education, financial transactions, and medical, criminal, or employment history.

ongoing); therefore content reviewers must consider not only the FOIA and the Privacy Act, but also the layers of federal, DoD, and Army regulation published since the national-emergency declaration¹³² for how **PII has become operational and sensitive information**. The federal laws – e.g., the FOIA and the Privacy Act – are foundational to DoD’s Web guidance, of course, but DoD and Army guidance can be more restrictive because of security considerations.¹³³

We’ve called PII a “special problem” because, as we said in Chapter 1, it’s impossible to tell the Army’s story without releasing PII, since the Army is people, but anyone with a modicum of Internet search skills can use just a name to compile a profile on a person using public-domain information. Therefore the goal of this section is to accomplish four things: 1) discuss the WWW’s dangers so that content reviewers will be better prepared to assess the release of PII; 2) clarify the sometimes-competing federal, DoD, and Army policies that TRADOC organizations are required to follow in releasing PII via their Websites; 3) provide TRADOC guidance on official command spokespersons and posting of biographies; and 4) make recommendations on adapting and applying OMB’s “best judgment” standard.

The WWW’s dangers. Beyond being *allowed* to be withheld under the FOIA and Privacy Act, subsequent DoD policy has *insisted* that PII be withheld because of increased risk to individuals. (See Footnotes 133 and 134.) DoD and Army policy have subsequently made a direct link between PII and other FOIA-exempt information as FOUO information¹³⁴ “because of the heightened interest in the personal privacy of DoD personnel that is concurrent with the increased security awareness demanded in times of national emergency.”

The Internet alone – and its associated conundrums of more computers per more world households, powerful WWW search abilities, better technology such as fiber-optics or wireless technology in more places, and the proliferation of Websites (and links) across the world – *guarantees* that there is an increased risk to individuals. On top of that, the wars and the enemies our country has incurred should cause us to pause before releasing PII without truly assessing its risks. Americans enjoy a free and open society, and have so infrequently experienced the dangers of sharing too much information, that we don’t recognize there is a downside – there is a **great deal of information that can be data-mined from the public Internet**: from Websites, Weblogs (blogs), YouTube, MySpace, Facebook, Reunion.com, etc. We give away more information than is necessary, and we give away information about ourselves that an adversary can use against us.

Every American citizen has adversaries. We are prey to cybercriminals, including identity thieves and other social engineers; to someone who means us harm because they don’t like our religion or politics, for instance; or to terrorists – Islamist terrorists, for example, have vowed to kill Americans just because we are Americans. So we must be aware that **our information will be aggregated to use against us**. Aggregation of information is the

¹³² The most recent version of AR 25-55, *The Department of the Army Freedom of Information Act*, which implements the federal law (the FOIA), is dated Nov. 1, 1997, with an update of Feb. 22, 2006, published in the *Federal Register*. The most recent version of AR 340-21, *The Army Privacy Program*, which implements the federal law (the Privacy Act), is dated July 5, 1985. The Open Government Act of 2007’s changes, if any, have not yet been reflected in AR 25-55 or AR 340-21.

¹³³ Organizations should consult their FOIA officer as a QI SME for this reason. IAW Paragraph 5-2c, AR 380-5, the FOIA provides that, for information to be exempt from mandatory release, it must fit into one of the qualifying categories, and there must be a legitimate government purpose served by withholding it. PII can be exempt from mandatory release under the “personal privacy” exemption, and DoD leaders have made it clear in various memoranda that the “legitimate government purpose” is protection of DoD personnel and their families, therefore PII is exempted from release on an organization’s publicly accessible Website via those memoranda. For other uses, simply because information is marked FOUO does not mean it automatically qualifies for exemption – if an organization receives a FOIA request for a record, the information must be reviewed to see if it meets the dual test of qualifying exemption and legitimate government purpose. On the other hand, the absence of the FOUO marking does not automatically mean the information must be released. Some types of records (for example, personnel records) are not normally marked FOUO but can still qualify for withholding under the FOIA. Organizations should not assume that the absence of the FOUO marking means the document is not FOUO.

¹³⁴ DoD changed the policy concerning release of PII in the pivotal OSD memorandum, “Withholding of Personally Identifying Information Under the Freedom of Information Act (FOIA),” Nov. 9, 2001: “Th[e] change in our security posture has implications for [DoD]’s policies implementing the [FOIA]. Presently all DoD components withhold, under 5 USC 552(b)(3), the [PII] (name, rank, duty address, official title and information regarding the person’s pay) of military and civilian personnel who are assigned overseas, on board ship, or to sensitive or routinely deployable units. Names and other information regarding DoD personnel who did not meet these criteria have been routinely released when requested under FOIA. Now, since DoD personnel are at increased risk regardless of their duties or assignment, . . . release of names and other personal information must be more carefully scrutinized and limited.” Also see the memo from ASD-C3I, “Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites,” Dec. 28, 2001, and Paragraph 4-100, Chapter IV, Section 1, AR 25-55.

phenomenon where information collectors and analysts take pieces of information and mold them into a useful profile of a person. An adversary aggregates because that's the first step for him to inflict harm: to learn where we may be weak. Therefore the adversary aggressively reads and collects material.

Collection of information usually begins with the Internet – an adversary will research the WWW to see how much information he can gather on us anonymously. He will study photographs and maps we post to the Web. Then he may conduct surveillance to confirm this information. Any little piece of PII we give away, inadvertently or on purpose, can be used by our adversaries.

A number of Websites in the public domain compile information on people. The following list includes some well-known Websites (there are others) a researcher could use to find out a person's addresses for the past 10 years; perform a background check for the past 20 years of a person's history; learn a person's current phone number and address; obtain an on-line map to that address; or learn a person's date of birth and ages, plus their relatives and their relatives' names and ages. For a fee ranging from \$3 to \$50 or so, it's possible to learn PII such as SSNs, bankruptcies, or civil and criminal court results.

- Zaba Search, www.zabasearch.com;
- Any Who, www.anywho.com;
- Know X, www.knowx.com;
- Lycos, www.lycos.com;
- The Public Records, www.ThePublicRecords.com;
- Intelius, www.intelius.com;
- People Look Up, www.PeopleLookUp.com;
- Web whitepages, <http://whitepages.addresses.com>;
- U.S. Search, www.ussearch.com;
- Pipl, www.pipl.com.

Therefore content providers and content reviewers should understand that when they decide, for instance, to identify a person in the public domain by his / her full name, that name can be used by an adversary to find the person's home address and telephone number. Websites like the Web whitepages enable reverse telephone number lookup to find a person's address. The Privacy Act and the FOIA have an impact on OPSEC, and vice versa.

Also keep in mind that disclosing information about a Soldier's degree of involvement in military actions in support of national policy, the type of military unit to which the member is assigned, and presence or absence from his or her household poses a security threat to the Soldier.¹³⁵

Federal, DoD, and Army policies for releasing PII via Websites. DoD and Army policies, in essence, have a blanket prohibition against releasing PII. We've seen that DoD and Army policy link PII to FOUO, and IAW DoD / Army policy, FOUO information will not be posted on publicly accessible Websites.¹³⁶ In addition to the DoD memos cited on the previous page, AR 25-1 states that Army organizations will not post on the Army's publicly accessible Websites "[PII] of personnel assigned within a particular component, unit, organization, or office in the DA."¹³⁷ (Traditionally, PII of personnel in overseas, "sensitive," or "routinely deployable" units was the only PII withheld, but these days, most Soldiers are assigned to units that are routinely deployed, so the release of all PII is more problematic.)

Following the preponderance of DoD and Army policy, TRADOC operates under the baseline standard that PII of lawful aliens and U.S. citizens in the following categories of personnel who are assigned to any TRADOC unit, organization, or office¹³⁸ is generally prohibited on the public Web; PII will be treated as FOUO information and therefore will be posted on public TRADOC Websites only after an OPSEC risk assessment by a certified HQ DA (Level II) OPSEC officer. This precaution is for publicly accessible Websites only; it isn't applicable to Websites that are PKI-enabled, adequately password-protected, or have other means of positive access control where the

¹³⁵ Paragraph K-12, Appendix K, AR 360-1.

¹³⁶ Paragraphs 3-3 and 3-6, Part II, DoD Web policy.

¹³⁷ Paragraph 6-7c(4)(i), AR 25-1.

¹³⁸ Memorandum from ASD-C3I, "Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites," Dec. 28, 2001.

public is prevented from gaining access to the information.¹³⁹ (Access and transmission controls are outlined in Chapter 4, the “Public Accessibility and Web Security” section.)

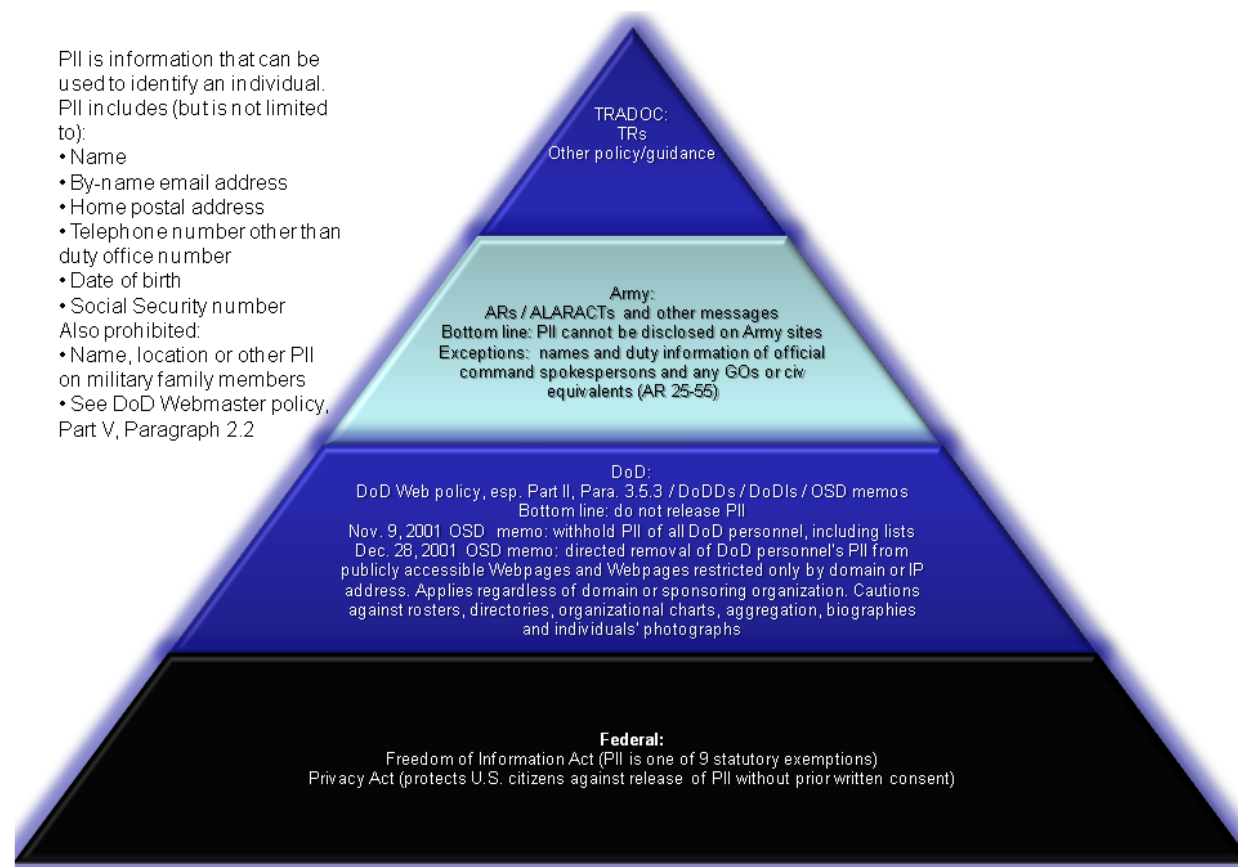


Chart 3-1. The PII pyramid. Policies and guidance governing release of PII build in levels based on the foundational federal law. Subsequent policy and guidance issued since the laws were passed, reflecting the national emergency (declared Sept. 14, 2001, and still ongoing), restrict the public release of PII.

The personnel categories are:

- Civilian employees;
- Active-duty military personnel;
- Contractors;
- Members of the Reserve Components;
- Coast Guard personnel when the Guard is operating as a service in the Navy; and
- Family members of all these categories.

The prohibition of PII applies to official Army Websites regardless of domain (e.g., .com, .edu, .org, .mil, .gov) or sponsoring organization (e.g., Morale, Welfare, and Recreation (MWR) sites or DoD educational institutions).

Some specific areas of DoD and Army PII policy follow.

Organizational directories made available to the public will list position titles rather than individuals' names.¹⁴⁰ Electronic versions of the directory may be placed on that organizational community page on AKO or AKO-Secure, but not on the publicly accessible Web. Even if placed in an AKO community area or other private Website, posting

¹³⁹ FOUO information is permitted if protected by PKI or other positive access control; see Table 1, Part V, DoD Web policy.

¹⁴⁰ Paragraphs 6-4r(1) and 6-4r(2), AR 25-1.

personal information (e.g., name, home address, or home telephone number) requires prior approval of the organization's Privacy Act and security officials.¹⁴¹

Lists of names of any personnel assigned to any component, unit, organization, or office within DA are prohibited.¹⁴² **Rosters, directories** (including telephone directories), and detailed **organizational charts** showing personnel are considered lists of PII and are prohibited, also IAW Army policy.¹⁴³ **Multiple names** of individuals from different organizations / locations listed on the same document or Webpage constitutes a list.¹⁴⁴

Organizations required to post **public contact information** (see "Required content" section, Chapter 4) should use organizational designation / title and generic position email addresses, such as office@organization.mil,¹⁴⁵ to avoid violating the Army's requirement to protect PII.

There are **four "automatic" exceptions to the prohibition of PII**:

- Names and duty information may be posted of personnel, who by the nature of their position and duties, frequently interact with the public.¹⁴⁶ These individuals are defined as official, designated **command spokespersons** and are GOs and SES members, PAOs, or other personnel designated as official command spokespersons.¹⁴⁷ At TRADOC CoE level,¹⁴⁸ the designation of official command spokespersons is usually the TRADOC senior commander (usually a brigadier general or major general), any GO-level deputy senior commander, and the TRADOC senior commander's PAO.
- Names and duty information may be posted of **any other GOs / SESs** within the command / activity.¹⁴⁹ Normally these GOs / SESs, because of their position and duties, will also be command spokespersons. (Even when allowed by these exceptions to the prohibition of PII, caution must still be exercised in aggregating key-leader names across multiple Webpages.)
- Command Websites may publish the **name, rank, and duty station of military personnel in PAO photo captions and news stories**.¹⁵⁰
- POC information on posted memoranda**, such as command-policy letters, is also excluded from the restriction on posting PII.¹⁵¹ (However, see the Privacy Act section, Page 34, for what precisely can be included in POC information.)

TRADOC guidance on command spokespersons and biographies. Since the PAO normally designates official command spokespersons on behalf of the commander, **PAO clearance / approval must be obtained to post all documents (including biographies) that contain names of those individuals who are not command spokespersons or who are not GOs / SESs**. This clearance / approval for non-command spokespersons must be applied for as

¹⁴¹ Paragraph 6-4r(2), AR 25-1. Approval from the organization's Privacy Act official and security official are required prior to posting personal information on AKO / DKO or other private Website. If posted on AKO / DKO, the information will be further restricted to those individuals with a need-to-know.

¹⁴² Paragraph 6-7c(4)(i), AR 25-1.

¹⁴³ Memorandum from ASD-C3I, "Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites," Dec. 28, 2001; TRADOC Command Guidance: Noble Eagle #02-019, "Personal Data on Unclassified Websites," March 13, 2002.

¹⁴⁴ Memorandum from ASD-C3I, "Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites," Dec. 28, 2001.

¹⁴⁵ Memorandum from ASD-C3I, "Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites," Dec. 28, 2001; TRADOC Command Guidance: Noble Eagle #02-019, "Personal Data on Unclassified Websites," March 13, 2002.

¹⁴⁶ Paragraph 6-7c(4)(i), AR 25-1.

¹⁴⁷ Memorandum from ASD-C3I, "Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites," Dec. 28, 2001; memorandum from OSD, "Withholding of Personally Identifying Information Under the Freedom of Information Act (FOIA)," Nov. 9, 2001; Paragraph 6-7c(4)(i), AR 25-1.

¹⁴⁸ Beyond HQ TRADOC, TRADOC consists of MSOs, CoEs, individual schools, field-operating activities (FOA), or other subordinate organizations that are involved in carrying out TRADOC's mission. (See "TRADOC subordinate organizations" in the definitions section for more details.) Hereafter in this *Guide*, these organizations may be referred to as "commands / activities," although they may be referred to as "mission activities" or other terminology in other documents. **TRADOC commands / activities are encouraged to parallel HQ TRADOC's Web Content Review Program as much as possible.**

¹⁴⁹ IAW AR 25-55, Paragraph 3-200, under exemption No. 6, "By DoD policy, the names of general officers (or civilian equivalent) or [PAOs] may be released at any time."

¹⁵⁰ Paragraph 6-7c(4)(i), AR 25-1.

¹⁵¹ Paragraph 6-7c(4)(i), AR 25-1.

exception to policy (with strong justification) and cleared for release by the TRADOC Chief of Public Affairs (CPA) (or TRADOC senior commander's PAO at the MSOs / CoEs), IAW regulations and guidance.

On a case-by-case basis, the TRADOC senior commander or TRADOC senior commander's PAO determines when others speak for the command – such as a colonel who serves as the commandant of a school within a CoE – and can be quoted in news stories or other public-information products, and therefore their names and duty information may also be released. This policy is designed to preclude the possibility of unit Websites becoming self-serving for leaders, whether officer or enlisted, and keep the sites oriented toward accomplishing a mission.

At HQ TRADOC, personnel not listed below **must** be officially designated as command spokespersons by the TRADOC CPA, who will determine that designation on a case-by-case basis by virtue of the person's subject-matter expertise for an event such as a news-media interview. The designation of command spokesperson expires upon completion of that event. Exceptions to this policy must be requested of the TRADOC CPA.

Posting of biographies, since they are PII, should be limited to command spokespersons and / or GOs / SESs (with considered exception, and justification permitted). Permitted biographies, however, must not include prohibited PII such as personal email address, home address, home telephone number, SSN, or date of birth, nor may they contain any reference to marital status or family members. Biographies that contain family information are security violations – enemies could use the information to threaten or harm family members and thus gain advantage by intimidating Soldiers.

All biographies, including GO / SES biographies or command-spokesperson biographies, must receive OPSEC and PAO review before they are posted.

Biographies are to be limited on the HQ TRADOC Website to the following official command spokespersons (unless an exception to the policy has been obtained from the TRADOC CPA):

- The TRADOC CG;
- The HQ TRADOC DCGs (DCG / Chief of Staff, DCG-Combined Arms, DCG-Initial Military Training (IMT), DCG-U.S. Army Reserve (USAR), and DCG-Army National Guard (ARNG));
- The ARCIC director;
- The TRADOC command sergeant major;
- The TRADOC CPA.

Biographies of other GOs / SESs may be posted by the organizations they are assigned to but, as stated, must receive OPSEC and PAO review before posting.

Noting the HQ TRADOC guidance above, a TRADOC senior commander should apply OPSEC measures to PII and limit the biographies posted to his / her command's Webpages to his / her official, designated command spokespersons and to any GOs / SESs in his / her command. Mission-side GOs / SESs, if not the same as the senior commander's staff, may have their names and duty information (including duty-related biographies) published as permitted by AR 25-55, but the TRADOC mission's senior command sergeant major's biography should be posted only if he / she serves as an official, designated command spokesperson under federal, DoD, and Army regulatory provisions. Further, NCO biographies, such as the commandant of the local NCO Academy, are not authorized as an exception to the policy unless the TRADOC senior commander's PAO specifically designates him / her as an official command spokesperson. Exceptions to this policy should be requested of the TRADOC senior commander's PAO and be accompanied by strong justification, which must be provided to content reviewers upon request.

TRADOC CoE Webpages must be differentiated from Installation Management Command (IMCOM) and other non-TRADOC command / activity Webpages. IMCOM's and other commands' / activities' critical, operational, and sensitive information is different than TRADOC's, so the OPSEC risk is different for TRADOC CoE Webpages; a sweeping, one-size-fits-all OPSEC risk assessment done for or by garrison activities cannot be applied to TRADOC – TRADOC Webpages must be considered on their own. With the OPSEC risk assessment in mind, TRADOC CoE homepages may elect to link to garrison / IMCOM or other command / activity Webpages that contain the garrison commander's biography and garrison sergeant major's biography, for instance. In addition, because TRADOC CoE Webpages are guided by a slightly different policy and exist for a different purpose than the garrison's mission, the Webpages belonging to the TRADOC CoE should be clearly distinguishable via some element of design from the garrison / IMCOM Webpages – at a minimum, a separate corporate template for all

pages belonging to the TRADOC CoE is recommended, to differentiate the TRADOC CoE's pages from the corporate template that IMCOM has standardized for garrison pages to use.

Summarized, the federal, DoD, Army, and TRADOC policy for PII is:

- In general, PII on all DoD personnel is not authorized and must be removed from publicly accessible Webpages. This applies to official, unclassified DoD Websites regardless of domain (.com, .org, mil, .gov) or sponsoring organization.
- If PII must be released, an OPSEC risk assessment must be completed first.¹⁵²
- Prohibited PII includes lists or rosters and directories (including telephone directories). Organizational charts showing personnel names are considered lists of PII. Multiple names of individuals from different organizations / locations listed on the same document or Webpage constitutes a list. Aggregation of names across Webpages must be specifically considered.
- By-name email addresses are considered PII. Sites needing to post contact information for the public should use organizational designation / title and generic email address accounts.
- PII on official, designated command spokespersons, including biographies that do not contain family member information, may be released. Official command spokespersons are discussed in preceding paragraphs. Exceptions must be requested of, and justified to, the TRADOC CPA.

OMB's best-judgment standard. We've discussed that PII of command spokespersons, any other GO / SES, certain information in photo captions and news stories, and POC info in memos is permitted, but can information about people not in these categories never be on the Web? What is the common-sense approach? Should PAOs designate everyone as official command spokespersons?

Under Army policy, it's not possible that everyone be a command spokesperson. However, PAOs may adapt the best-judgment standard outlined in OMB M-07-16 to decide whether or not to release an individual's name. (*Caveat:* The best-judgment standard doesn't apply to lists, only to single names, which are sensitive in context. For example, one Army rule is to not post lists of names, as outlined above; including a number of names in a single journalism story may constitute a list and therefore the best-judgment standard cannot be applied, but the OPSEC-review methodology must be.)

The best-judgment standard of OMB M-07-16 contains guidance on when PII *breaches*¹⁵³ should be reported. When reported, the breach may be determined an *incident*.¹⁵⁴ People who discover PII *compromises* are responsible for reporting it if PII is potentially or actually compromised. *Breaches, incidents, and compromises* have more to do with a network's physical security; for our purposes here, PAO, as the proponent for information released into the public domain, should think in terms of whether release of the PII would be reported as *logical access* per OMB M-07-16 – and if so, it makes sense to not release something that would be considered a breach. Per OMB M-07-16, an incident report does not have to be filed in every case of a PII breach; those cases are outlined in the OMB document, and a best-judgment standard is applied to determine whether an incident report must be filed. TRADOC PAO recommends that PAOs adapt OMB M-07-16's best-judgment approach to help determine whether to release an individual's name once the OPSEC officer's assessment is obtained. The best-judgment standard can also be considered in an organization's request to the TRADOC CPA for an exception to the policy prohibiting release of a single, individual name (which is PII) when that person is not an official command spokesperson or GO / SES.

However, in considering PII, there are *minimum yardsticks*; PII must be assessed by *loss impact*¹⁵⁵ and *sensitivity*.¹⁵⁶

¹⁵² Paragraph 4-20g(11), AR 25-2, et al.

¹⁵³ Per OMB M-07-16, a *breach* is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other-than-authorized purposes have access or potential access to PII, whether physical or electronic. Of note is that the definition of *access* is more broad than in common network / server usage; *access* is the ability or opportunity to gain knowledge of PII.

¹⁵⁴ Potential and confirmed breaches are reported as *incidents* when an individual gains *logical* or *physical access* without permission to a federal agency's network, system, application, data, or other resource; or if there is a suspected or confirmed breach of PII regardless of the manner in which it might have occurred.

¹⁵⁵ Potential *impact* on one's organization is assessed on whether the loss will keep the organization from accomplishing its assigned mission, protecting its assets, fulfilling its legal responsibilities, maintaining its day-to-day functions, or protecting individuals. Loss of PII may involve several of those categories.

¹⁵⁶ *Sensitivity* of PII is determined by context. A single name that appears on a list of patients at a clinic for treating contagious disease can incur significant harm – this is an example of where a name in one context is more sensitive than in another.

PII loss impact is judged on three levels: low,¹⁵⁷ moderate,¹⁵⁸ and high.¹⁵⁹ In most cases, PAO is most concerned whether there will be harm¹⁶⁰ to the individual – and, in some cases, harm to the organization – in determining whether to release PII; if there is little or no risk¹⁶¹ of harm, removing the single, individual name from the Web might create unnecessary concern and confusion. However, PAO personnel must balance this against OMB M-07-16's requirement that loss of PII must be categorized as moderate or high impact. Before applying *best judgment* in determining if PII such as a name should be released or reported – or even if that name needs to be removed from the Web as too sensitive – PAOs must assess the likelihood that the breach may lead to harm. The assumption must be that potential or actual loss of PII can lead to at least significant harm, per OMB M-07-16.

Also, part of the loss-impact assessment is the organization's ability to mitigate the harm's risk. Obviously, some harm is more difficult to mitigate than other harm. In the case of harm to individuals, releasing information into the public domain is impossible to mitigate – once released, it's out of the releaser's control.

Therefore, in applying *best judgment*, assess 1) the likely risk of harm; 2) the level of risk; 3) the likelihood that the breach leads to harm; 4) the likelihood harm will occur; and 5) the mitigation of risk. We recommend that PAOs discuss this with their G-6s. If there is a thorough OPSEC assessment according to current methodology, and if PAO personnel apply *best judgment* – adapting the Federal Information Processing Standard (FIPS) 199 and FIPS 200 standards cited in OMB M-07-16 for PII breaches – then the benefits of telling that individual's story, and therefore releasing that individual's name, may outweigh any potential disadvantages. But PAO personnel must ensure that the OPSEC and best-judgment assessments are performed; releasing PII into the public domain, especially on the Web, is not "business as usual" – the section on how dangerous the WWW can be should have demonstrated that. The results of the best-judgment application in requests for the TRADOC CPA to grant exception to policy must be justifiable.

Another "standard" in determining whether logical loss of PII from a Website could be a breach and therefore reportable is to determine if the event / incident of loss may be of concern to TRADOC's CG. The factors determining the TRADOC CG's interest are given in TR 1-8 as severity of the event / incident, potential

¹⁵⁷ Low impact means that there is *limited adverse effect* on organizational operations, organizational assets, or individuals.

Limited adverse effect means that there is degradation in mission capability, but the organization is able to perform its primary functions; the effectiveness of the organization's functions are noticeably reduced; there is minor damage to organizational assets; there is minor financial loss; and / or there is minor harm to individuals. (OMB M-07-16 and FIPS 199)

¹⁵⁸ In moderate impact, there is *serious adverse effect* on organizational operations, organizational assets, or individuals. *Serious adverse effect* is significant degradation in mission capability; the organization is able to perform its primary functions, but the effectiveness of those functions is significantly reduced; there is significant damage to organizational assets; there is significant financial loss; and / or there is significant harm to individuals that does not involve loss of life or serious life-threatening injuries. The loss impact of PII is, at minimum, of moderate impact, where there can be substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is obtained. (OMB M-07-16 and FIPS 199)

¹⁵⁹ High impact means there is a *severe or catastrophic adverse effect* on organizational operations, organizational assets, or individuals. *Severe or catastrophic adverse effect* entails severe degradation in, or loss of, mission capability so that an organization is not able to perform one or more of its primary functions; major damage to organizational assets; major financial loss; and / or severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries. (OMB M-07-16 and FIPS 199)

¹⁶⁰ Harm is defined in OMB M-07-16 as damage, fiscal damage, or the loss / misuse of information which adversely affects one or more individuals or undermines the integrity of a system or program. PAO personnel must consider a wide range of harms, such as harm to reputation and the potential for harassment or prejudice, particularly if health or financial-benefits information is involved. There is a broad definition to *potential harm*, and it includes embarrassment, inconvenience, or unfairness. The effect of a breach, for example, may be the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or unwarranted exposure leading to humiliation or loss of self-esteem. The likelihood harm will occur depends on the manner of the breach and the type of information involved, such as SSNs, bank account information, date of birth, passwords, or mother's maiden name, which are useful in identity theft.

¹⁶¹ Risk is defined in FIPS 200 as the level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. The assessment of risk here is not the OPSEC risk assessment; this assessment is specific to FIPS 199 and FIPS 200 standards and looks at the vulnerability of the organization's information systems, system-security procedures, internal controls, or implementation that could be exploited or triggered by a threat.

consequences of the event / incident, and potential for publicity.¹⁶² TRADOC organizations are to report all incidents of lost, stolen, or compromised PII in both electronic and physical form.¹⁶³

In general, DoD and Army policy provide a good benchmark, keeping in mind the policy discussed previously:

- Personnel should only **collect** personal information that is relevant, legally authorized, and necessary to support Army operations, or is required by federal statute or presidential EO.¹⁶⁴ PII will be collected to the greatest extent practicable “directly from the individual.”¹⁶⁵ (*Relevant* is an especially good benchmark to use when collecting PII for use in CI news stories.)
- Personnel will only **disclose** personal information as “relevant and necessary” to accomplish a lawful DoD purpose. Personal information shall be **relevant, timely, complete, and accurate** for its intended use.¹⁶⁶
- Personnel must **safeguard** PII to prevent unauthorized use, access, disclosure, alteration, or destruction.¹⁶⁷ Personnel, including contractors, have an affirmative responsibility to protect an individual’s privacy when collecting, maintaining, using, or disseminating anyone’s PII.¹⁶⁸
- Disclosure of records pertaining to personnel of **overseas, sensitive, or routinely deployable units is strictly prohibited**.¹⁶⁹ (Also see DoD Web policy.)

For assistance in assessing harm and risk, see the “Loss-of-PII Consequence Table” at the end of this chapter.

ROLES AND RESPONSIBILITIES FOR REVIEWERS

Many of the references in Chapter 1 requiring Web-content review also spell out what those reviews will require. Content review will be for: 1) sensitivity, including FOUO information;¹⁷⁰ 2) format;¹⁷¹ 3) required content restrictions and inclusions;¹⁷² 4) privacy;¹⁷³ 5) OPSEC;¹⁷⁴ 6) the Website-management control checklist (Appendix C, AR 25-1) as a minimum review;¹⁷⁵ and 7) information quality.¹⁷⁶ This entails the reviewers as listed in Chapter 1: OPSEC / security, Webmaster, and QI. SJA review in certain instances is required by other references. IAW Army policy, all content posted to the Web must have OPSEC and PAO review *before* it is posted, even if it is cleared by another government agency, because content can become sensitive upon compilation.¹⁷⁷

Because of the many requirements, content reviews should be conducted IAW the following sections – plus the “content-review procedures” section later in this chapter – and any subsequent DoD, Army, or TRADOC policy and guidance published after this *Guide* is published, to ensure that all DoD, Army, and TRADOC policy and procedures are followed. The pre-dissemination review procedures checklist at the end of Chapter 2 should also

¹⁶² Paragraph 2-1a, TR 1-8.

¹⁶³ See TRADOC memo “Reporting the Loss of Personally Identifiable Information) and Paragraph 3-1d, TR 1-8. Losses are to be reported to the U.S. Computer Emergency Response Team (US-CERT) and the DA Freedom of Information Privacy Act Office within one hour of discovery. Also refer to Paragraph 4-21d, AR 25-2; loss of some PII may require a serious incident report (SIR) per AR 190-45. These are the conditions necessitating a SIR: 1) the incident poses grave danger to the Army’s ability to conduct established information operations; 2) the incident is causing / will cause adverse effects on the Army’s image (e.g., Webpage defacements; 3) there is access or compromise of classified, sensitive, or protected information such as Soldier identification information (e.g., SSN), medical condition or status, doctor-patient, or attorney-client privilege; or 4) there is compromise of systems that may risk safety, life, or limb; may have the potential for catastrophic effects; or may contain information for which the Army is attributable.

¹⁶⁴ Paragraph 4.2.1, DoDD 5400.11; Paragraphs 1-5b and 4-1c, AR 340-21.

¹⁶⁵ Paragraph 4.2.2, DoDD 5400.11; Paragraphs 1-5b and 4-1d, AR 340-21.

¹⁶⁶ Paragraph 4.2.3, DoDD 5400.11; Paragraph 1-5c, AR 340-21.

¹⁶⁷ Paragraph 1-5d, AR 340-21.

¹⁶⁸ Paragraph 4.1.3, DoDD 5400.11.

¹⁶⁹ Paragraph 4.7, DoDD 5400.11; Section 505.7, 32 CFR, *The Army Privacy Program*.

¹⁷⁰ See DEPSECDEF memo, “Department of Defense (DoD) Website Security Policy Compliance,” Sept. 25, 2008.

¹⁷¹ DEPSECDEF memo cited in ALARACT “Website Security Policy Compliance.”

¹⁷² DEPSECDEF memo cited in ALARACT “Website Security Policy Compliance”; SecArmy’s executive-summary response to the DEPSECDEF’s tasking in “Department of Defense (DoD) Website Security Policy Compliance,” Sept. 25, 2008.

¹⁷³ Ibid, both sources.

¹⁷⁴ Ibid, both sources.

¹⁷⁵ Paragraph 6-7c(4), AR 25-1; SecArmy’s executive-summary response to the DEPSECDEF’s tasking in “Department of Defense (DoD) Website Security Policy Compliance,” Sept. 25, 2008.

¹⁷⁶ Paragraph 6-7c(6)(b), AR 25-1.

¹⁷⁷ Paragraph 5-4a, AR 360-1.

assist in the content-review process; although the checklist is primarily a tool for content providers, both content reviewers and organizational Website coordinators (see Chapter 4) could benefit from its use in ensuring that all reviews are accomplished before submitting the content to PAO for approval / clearance to post. Checklists for all types of reviewers are included at the end of this chapter to help ensure that reviews are thorough.

The following section outlines the roles and responsibilities of the content-reviewer cadre in TRADOC's Web Content Review Program. The content-review procedures themselves are included later in this chapter. Procedures prescribed by DoD Web policy are at Appendix K.

REVIEWER ROLES AND RESPONSIBILITIES: ORGANIZATIONAL WEBMASTER

One of the organizational Webmaster's major roles is "lookin' out" for the network. The Federal Information Security Management Act (FISMA) requires federal agencies to provide information-security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information maintained on the agency's information systems. Fulfilling the requirements for establishing and maintaining security and access controls based on the information's sensitivity and on the target audience for which the information is intended can be a full-time job. Organizational Webmasters must also apply the appropriate privacy and security policies to respect visitors' privacy.¹⁷⁸ However, the Webmaster also is charged to review content quarterly and may use Web-analysis software to complete his / her review.¹⁷⁹

Much of the organizational Webmaster's work for our purposes here is in the pre-dissemination review process. Organizational Webmasters:

- Advise content providers on design and network / bandwidth issues;
- Coordinate with the TRADOC Webmaster if the organization's content will affect TRADOC's network;
- Perform Webpage testing for functionality and Section 508 compliance (see Appendix N for more discussion on Section 508 compliance standards);
- Make the initial determination on how to apply the appropriate access and security controls for content IAW Paragraph 3, Part II, and Table 1, Part V, of the DoD Web policy;
- Verify that a QI review of the information has been accomplished within the organization as part of the "verification" step of Paragraph 3, Part II of the DoD Web policy;
- Validate all hyperlinks from the information before posting it as part of their own QI review;
- Work with content providers to ensure that metatags are included with each Webpage (see Chapter 2); and
- Post their organization's information once it clears the review process.

Organizational Webmasters may use the Webmaster's review procedures and policy checklists for assistance in conducting their reviews. Both checklists are found at the end of this chapter.

REVIEWER ROLES AND RESPONSIBILITIES: OPSEC OFFICER

Because the Army's primary OPSEC vulnerability is information made publicly accessible through Websites and Web-enabled applications,¹⁸⁰ the organizational OPSEC officer reviews all content to be placed on a TRADOC

¹⁷⁸ Paragraphs 5-1, 6-7a(12), and 6-7c(5), AR 25-1.

¹⁷⁹ Paragraph 6-7c(4), AR 25-1.

¹⁸⁰ Paragraph 3-3i, AR 25-2. Also, see Paragraph 5-2d(1), AR 530-1: "The OPSEC Website review is the responsibility of the Webmaster, in coordination with the OPSEC officer, ... PAO and other appropriate designees (security and intelligence, command counsel, and so forth)." However, TRADOC's approach is that the quarterly OPSEC Website review (post-dissemination review) is both the organizational OPSEC officer's and the organizational Webmaster's responsibility. If the Webmaster is not certified in Web OPSEC content IAW the training requirements of ALDODACT 11/06 and the TRADOC OPSEC Program (Level II, or HQ DA certification, is required, per the TRADOC OPSEC officer in an email dated April 9, 2009), the organizational OPSEC officer accomplishes the review alone until the organizational Webmaster can be trained to standard. (See Chapter 6 for training requirements and recommendations.) This applies to information already posted; the organizational OPSEC officer is solely responsible for the pre-dissemination OPSEC review of documents IAW AR 530-1. Also, the TRADOC OPSEC Action Plan's Goal 12 requires that the quarterly review "[a]ssess ... what OPSEC violations there are, nature of the violations (trends) and feedback getting from field" – although responsibility for this assessment is primarily TRADOC PAO's, organizational OPSEC officers and organizational Webmasters should provide input to it.

Website for OPSEC-sensitive information, as well as conducts quarterly reviews to ensure that no OPSEC concerns have crept into Web content. OPSEC focuses on identifying and protecting the organization's unclassified information that may individually or in the aggregate lead to the compromise of classified information and sensitive activities. An OPSEC content review is an evaluation of information intended for release outside the control of the organization, including release to the public.¹⁸¹

By now, it should be well-established that not all content is appropriate for the publicly accessible Web. OPSEC reviewers help determine whether the content provider's proposed content should be public or non-public, based on the information's sensitivity and its target audience, as well as the level of risk to DoD interests. Organizational OPSEC officers and organizational security managers should work together to achieve and maintain *essential secrecy* for their organizations.

OPSEC review is a big job if done right. The actual five steps of the OPSEC analysis are contained in AR 530-1 and in Appendix 1 to Enclosure 3, DoD Manual 5205.02-M, but for our purposes here, we'll discuss the areas an organizational OPSEC officer should assess while keeping in mind all Web-content requirements.

Organizational OPSEC officers:

- Perform OPSEC review on the organization's documents as established in the organization's SOP and IAW AR 530-1. OPSEC is a process of five steps developed to deny adversaries publicly available indicators that are generally unclassified. OPSEC review identifies, analyzes, and protects *critical information*, which is information about friendly activities, intentions, capabilities, or limitations that an adversary needs to gain a military, political, diplomatic, or technological advantage.¹⁸² (See Appendix E for examples of critical information.) In the five steps, an organizational OPSEC reviewer identifies critical information; then conducts a threat analysis (with the aid of the organizational security manager), a vulnerability analysis, and a risk assessment; then recommends what OPSEC *countermeasures* to apply: release the information to the Web as is (no countermeasures), release the information to the Web with modifications, or don't release the information to the Web.
- Review the organization's information and visual content proposed for release in any public domain to ensure protection of critical or *sensitive information*.¹⁸³ (See Appendix I for examples of sensitive information.) Vulnerabilities can be eliminated by actively reviewing Web content from the perspective of what may be helpful to an adversary prior to posting any information to the Web.¹⁸⁴ *Critical and sensitive information may not be placed on a Website that is accessible to the public.*¹⁸⁵
- Examine submitted information for the presence of *any information requiring protection*, such as the examples listed in Appendices E through J, or other information qualifying as exempt from public release.
- **Review information IAW AR 530-1:**
 - **Screen proposed content for PII.** (See Appendix J for a list of PII.) PII is a category of sensitive information that is especially vulnerable. Lists of names and accompanying sensitive information of personnel assigned to a unit, organization, or office in DA are prohibited on the WWW. A single individual's name may be sensitive in context.¹⁸⁶ (See discussion on PII earlier in this chapter.) However, discretionary release of names and duty information of personnel who frequently interact with the public by nature of their positions and duties – such as general officers and senior executives, PAOs, or other personnel designated by PAO as official command spokespersons – is permitted.¹⁸⁷

The OPSEC reviewer's assessment should *consider PII under the categories of CUI, FOUO, and sensitive information, as well as being possible critical information.*

- **Assess the risk on any FOUO information.** FOUO information is information, the disclosure of which would cause a foreseeable harm to an interest protected by one or more of the exemptions

¹⁸¹ Enclosure 5, DoD Manual 5205.02-M.

¹⁸² Glossary, CJSI 3213.01B; Paragraph 5-1, AR 530-1.

¹⁸³ Paragraph 2-1c, AR 530-1.

¹⁸⁴ ALARACT message, "Army-wide Website OPSEC Review," Feb. 28, 2003.

¹⁸⁵ Paragraph 5-2d, AR 530-1.

¹⁸⁶ OMB M-07-16.

¹⁸⁷ Paragraph 1-5c(3)(d), AR 530-1.

to the FOIA. DoD policy prohibits FOUO on the publicly accessible Web, but there may be exceptions that the OPSEC officer will be called upon to review / assess.

If the OPSEC reviewer's assessment determines that the overall risk in posting the information to the publicly accessible Web is unacceptable, the organization may be permitted to post information in non-publicly accessible intranet areas which must have adequate security and access controls¹⁸⁸ as described in Chapter 4's "public accessibility and Web security" section. The **minimum security and access control for posting FOUO information is PKI client / user authentication**, IAW DoD Web policy.¹⁸⁹

Exceptions to the no-FOUO-on-the-public-Web policy can be submitted to reviewing officials for consideration for public release, but the request for exception must be accompanied by a **formal risk assessment** IAW this paragraph: "A formal risk assessment shall be conducted ... based on the value of the information; the threat to the DoD Webserver environment and the information contained thereon; and the countermeasures employed by the DoD Webserver environment."¹⁹⁰ In cases where the content is a risk to persons and not to a DoD Webserver, the risk assessment will focus on the value of the information.

However, in addition to the formal risk assessment and request for exception to policy, FOUO may not be released to the public without undergoing a **FOIA and legal review**; the OPSEC reviewer should coordinate with the G-6's FOIA officer and SJA, as well as with PAO, if FOUO is proposed for release to the public.¹⁹¹

Also, while records containing FOUO information are normally marked so at the time they are created, the OPSEC reviewer must **not assume that records without FOUO markings do not contain FOUO information**. The OPSEC reviewer will also remember that "[r]elease of information under the FOIA can have an adverse impact on OPSEC"¹⁹² and will assist the FOIA officer in determining whether to release information under the FOIA.

Special attention must also be given to identifying information that would **facilitate circumvention** of DoD, component, or command policies, rules, regulations, or other significant guidance (e.g., orders, manuals, instructions, or SCGs). Such information should be marked FOUO and will not be posted to publicly accessible Websites.¹⁹³

Special attention must also be given to the **increased sensitivity of information**, even if not FOUO, **if it can be electronically aggregated** in significant volume.¹⁹⁴ Information in electronic format may be data-mined.¹⁹⁵ **Aggregation of names across pages** must specifically be considered; as discussed in the "special problem of PII" section earlier in this chapter, name data can be compiled easily using simple Web searches. If aggregation of lists of names is possible across a single organization's Website / pages, that list should be evaluated on its merits and the aggregated elements treated accordingly.¹⁹⁶ OPSEC reviewers should keep in mind these words: "The Web can ... provide our adversaries with a potent instrument to obtain, correlate, and evaluate an unprecedented volume of aggregated information regarding DoD capabilities, infrastructure, personnel, and operational procedures. Such information, especially when combined with information from other sources, increases the vulnerability of DoD systems and may endanger DoD personnel and their families."¹⁹⁷

- **Review photographs intended for posting to the organization's Website to screen photographs displaying critical or sensitive information.** Examples of sensitive photos include, but are not limited to, IED strikes; battle scenes; casualties; destroyed or damaged equipment; personnel KIA, both friendly and adversary; and the protective measures of military facilities.¹⁹⁸ See Appendix I, "photographs" entry, for more information.

¹⁸⁸ Paragraph 3.5.2.3, Part II, DoD Web policy.

¹⁸⁹ See Table 1, Part V, DoD Web policy.

¹⁹⁰ Paragraph 5.2, Part II, DoD Web policy.

¹⁹¹ Paragraph 1-5c(3)(e), AR 530-1.

¹⁹² Paragraph 5-100c, AR 25-55.

¹⁹³ ALDODACT message 11/06.

¹⁹⁴ Paragraph 2, Part V, DoD Web policy.

¹⁹⁵ Paragraph 3.5.2 and 3.5.2.1, Part II, DoD Web policy. Also see memorandum from the DEPSECDEF, "Operations Security Throughout the Department of Defense," Oct. 18, 2001: "Unclassified information may ... need protection because it can often be compiled to reveal sensitive conclusions."

¹⁹⁶ Memorandum from ASD-C3I, "Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites," Dec. 28, 2001.

¹⁹⁷ Memorandum from the DEPSECDEF, "Information Vulnerability and the Worldwide Web," Sept. 24, 1998.

¹⁹⁸ Paragraph 2-1c, AR 530-1.

- Screen proposed content for critical or sensitive information that has **already been compromised**, as this provides further unnecessary exposure of the compromised information and may serve to validate it.¹⁹⁹
- Conduct **quarterly reviews** of the organization's Website for possible critical or sensitive information already posted. Per DA policy, the minimum review will include all Website management control checklist items in AR 25-1, Paragraph C-4e,²⁰⁰ but TRADOC PAO also recommends that the OPSEC / security reviewer's checklist at the end of this chapter be used, as it is tailored specifically for OPSEC Web-content reviewers. As mentioned, TRADOC PAO also recommends use of Appendices E through J, which list examples of critical information, CUI, FOUO information, OPSEC indicators, sensitive information, and PII.
- In conjunction with the organizational security manager, review official information intended for public release pertaining to **military matters, national-security issues, or subjects of significant concern** to DoD, IAW DoDD 5230.9 and DoDI 5230.29.²⁰¹ (See Appendix K.) This includes information regarding military operational plans.²⁰²
- Consult the organization's security manager if presented with **unclassified information pertaining to classified programs**. (Keep in mind that the security review is not the same as the OPSEC review;²⁰³ the security review protects classified information, while OPSEC protects critical and / or sensitive information, including FOUO information, which by definition is unclassified.)

Special attention must be given to unclassified information pertaining to classified programs. If this type of information is proposed for posting to a publicly accessible Website, reviewers should consider if there is a likelihood of **classification by compilation**. Reviewers should consult the program SCG to determine the likelihood that the information, if compiled or aggregated with other information likely to be posted on publicly accessible Websites, will reveal an additional association or relationship that meets the standards for classification under DoD 5200.1-R.²⁰⁴ If so, the information may be posted only if protected by a client / user authenticator IAW the security and access controls specified in Table 1, Part V, of the DoD Web policy.²⁰⁵ Also, since there are levels of classification most computer systems are not certified to process, TRADOC PAO recommends consultation with the organization's IT experts.

OPSEC and security reviewers should use advanced search engines (for example, high-end natural-language-based systems optimized for English syntax analysis) and other automated means to help assess whether the likelihood of information already on the public Web will cause the proposed information to become classified by compilation.²⁰⁶

As we said, it's a big job to accomplish OPSEC review if it's done right, but it may aid an OPSEC reviewer in his / her assessment to consider categories of information as "**fences**" that help prohibit certain types of information from being posted on the public-domain Web – i.e., the reviewer can mentally check off if the content he / she is reviewing contains any of these types of information. The fences, several of which overlap, are:

- OPSEC indicators;
- Sensitive information (which includes FOUO);
- CUI (which also includes FOUO); and
- Critical information.

Special attention must be paid to three other fences:

- Photographs;
- Only releasable by OSD;

¹⁹⁹ Paragraphs 2-2 and 1-5d(2), AR 530-1.

²⁰⁰ Paragraphs 2-3a(15) and 5-2d(1), AR 530-1.

²⁰¹ Also see ALDODACT message 11/06; message from the SECDEF, "Website OPSEC Discrepancies," Jan. 14, 2003; Paragraph 5-1, AR 360-1.

²⁰² ALDODACT message 11/06.

²⁰³ Paragraph 3 of Enclosure A, CJCSI 3213.01B; Paragraphs 1-6b and G-1, AR 530-1.

²⁰⁴ Paragraph 3.5.4, Part II, DoD Web policy.

²⁰⁵ Ibid.

²⁰⁶ Paragraph 3.5.4.3, Part II, DoD Web policy.

- National-security information (overlaps with OSD-only-releasable).

OPSEC indicators. TRADOC PAO recommends that OPSEC reviewers use Appendices E through J in this *Guide* for reference, but especially to consult Appendices H and I, for content defined variously as sensitive, FOUO, CUI, and critical information; these categories, as well as Appendix H, also contain OPSEC indicators. Check content for information about military facilities, including location, units, weapons used, fortifications and tunnels, amount of lighting, exterior size and shape, number of personnel, ammunition depot locations, leave policies, brigades and names of companies, or degree and speed of mobilization.

See Part V of the DoD Web policy; Paragraph 1-5, Appendix C, and Appendix D, AR 530-1; and Appendix C, AR 25-1, for more information.

Sensitive information – types of. See Appendices G and I for specifics. Categories of sensitive information include:

- FOUO (e.g., PII; proprietary information; test and evaluation information; technical information; information that would facilitate circumvention of DoD, component, or command policies, rules, regulations, or other significant guidance; unclassified information that requires special handling; documents or information protected by a copyright; and draft publications such as policies and regulations);
- Unclassified technical data;
- Department of State's (DoS) SBU information; or
- Foreign government information.

For more information, see the DoD Web policy and AR 380-5.

CUI. See Appendix F. For more information, see AR 380-5.

Critical information. See Appendix E.

Photographs. These are the organizational OPSEC officer's tasks involving **photography, multimedia, and other imagery**:

- Review **single photographs**, especially photos depicting the subjects in Appendix I, "photographs" entry, for OPSEC indicators, such as if the Soldier's unit patch is included in the photo. Review **photo captions** for possibly critical information, such as if the person's unit or unit mission is given in the caption or if details are provided on how the unit communicates. Consider recommending to content providers who want to post photographs to replace any "close-ups" of personnel with longer-range shots that would show no clearly identifiable faces, nametags, or unit patches.

Exercise caution with photographs because the enemy is searching for them on the Internet to obtain **targeting data or propaganda fodder**. A message from the Army Vice Chief of Staff (VCSA) labeled as "sensitive" any photos that show the results of IED strikes, battle scenes, casualties, destroyed or damaged equipment, and enemy KIAs. "Insurgents often use Websites to communicate, train, and recruit followers, often using photos / video of their battlefield successes," the VCSA message stated. "We cannot afford to have our photos become training and recruitment tools for the enemy. ... Moreover, we must protect information that may have a negative impact on foreign relations with coalition allies or world opinion."²⁰⁷ Particularly vulnerable to enemy exploitation are photographs that disclose weapons-systems vulnerabilities and friendly tactics, techniques, and procedures (TTP).²⁰⁸

Other types of photographs – in addition to the categories the VCSA outlines – which Army publicly accessible Websites must not post include (but are not limited to): **equipment vulnerabilities, intelligence-collection efforts and methods, or the protective measures of military facilities**. Photographs of **ongoing friendly operations** must be carefully considered. Also, recent OPSEC analysis indicates that adversaries are looking for footage (clips, photos, etc.) of Soldiers taken from **within U.S. bases**.

²⁰⁷ ALARACT message, "Sensitive Photos," Feb. 14, 2005. See also Paragraph 2-19, AR 530-1, and Paragraph 6a(6), TRADOC OPSEC Plan: "Be aware of the vulnerabilities exposed as a result [of] the disclosure of sensitive and critical information on the Internet. In particular, avoid disclosure of photos showing the results of IED strikes, battle scenes, casualties, destroyed or damaged equipment, enemy KIAs, and access to military facilities."

²⁰⁸ ALARACT message 156/2005, "Chief of Staff of the Army OPSEC Guidance," Aug. 23, 2005; ALARACT message, "Sensitive Photos," Feb. 14, 2005.

- Beware of **photo backgrounds**, which may seem innocuous; good photo-editing software can magnify the background information enough to where an adversary can learn information from background walls, easels, computer screens, etc.
- Also consider **sequential photos**. We recommend that OPSEC reviewers advise those who wish to post photographs to delete the photo's background (or crop it closely) and to not post sequential photos.
- Review **directories or collections of photographs** for risk in the aggregate. If the organization's on-line photo library is determined to be a risk, the organization must move the collection of photographs to a private Webserver and protect it by adequate security / access controls.
- Review the organization's **multimedia / VI products** for any still photography of prohibited subjects.

Only releasable by OSD. IAW Paragraph 5-3, AR 530-1, information that meets any of the following criteria must be submitted to the Army's Office of the Chief of Public Affairs (OCPA)²⁰⁹ through TRADOC PAO for OSD clearance prior to release, as it most likely qualifies as **national-security information**. (DoDI 5230.29 will also apply for these criteria.) In fact, OSD will probably reserve to itself the prerogative to release this sort of information, as it normally releases general military information on the overall plans, policies, programs, or operations of DoD, DA, or the federal government.²¹⁰ At minimum, since OCPA has the sole authority to release information about the Army as a whole,²¹¹ it would not be appropriate for these types of information to be released at ACOM level or below.

Doubtful cases must also be submitted for clearance. Prior unofficial publication of information does not constitute authority for official release.²¹²

Where there is overlap with Enclosure 3, Paragraph 1, DoDI 5230.29 – which is the list of types of information that must be submitted to DoD's Office of Security Review (OSR) for review before release – that is noted in the following list:

- Information that originates from or is proposed for release at the **seat of government** (also corresponds to DoDI 5230.29, which adds "by senior personnel on sensitive political or military topics");
- Information that is or has the potential to become an item of **national or international interest** (also corresponds to DoDI 5230.29);
- Information and public statements with **foreign-policy or foreign-relations implications** (corresponds to DoDI 5230.29; also – and first – coordinate with HQ TRADOC's foreign-disclosure (FD) officer (in G-2) or the MSO's FD officer);
- Information and public statements concerning **high-level military or DoD policy**;
- Information concerning **U.S. government policy** or **policy within the purview of other government agencies**;
- Information **approved by HQDA for release by OSD**;
- Information on subjects of **potential controversy among the military services or with other federal agencies** (also corresponds to DoDI 5230.29);
- Initial information on **new weapons or weapon systems or significant modifications or improvements to existing weapon systems, equipment or techniques** (corresponds to DoDI 5230.29; also consult TRADOC G-2's FD officer or the MSO FD officer);
- Information on **significant military operations, potential operations, OPSEC, and military exercises** (also corresponds to DoDI 5230.29);
- Information on **military applications in space** (also corresponds to DoDI 5230.29);

²⁰⁹ IAW Paragraph 6-6a, AR 360-1, HQ DA and OSD clearance is required for communications products containing information meeting the criteria outlined in Paragraph 5-3, AR 360-1 – the same categories noted above. Per Paragraph 6-9b, AR 360-1, these materials must be submitted to OCPA. TRADOC PAO will assist in getting the materials to OCPA. Submission procedures are also outlined in Paragraph 6-9b, AR 360-1.

²¹⁰ Paragraph 5-3a, AR 360-1.

²¹¹ Paragraph 5-3b(1), AR 360-1.

²¹² Paragraph 5-3a, AR 360-1.

- Information on **weapons of mass destruction** (including nuclear weapons) and the components of such weapons (also corresponds to DoDI 5230.29), including:
 - **Nuclear**-weapons-effects research;
 - **Chemical warfare** and defensive **biological** and toxic research;
 - High-energy **lasers** and **particle-beams** technology.
 - **Nuclear, biological and chemical** (NBC) defense testing and production, policies, programs, and activities;
- Information on **national command authorities** (NCAs) and NCA command posts;
- Information and materials, including submissions by defense contractors, involving **critical military technology**;
- Information concerning **communications security** (COMSEC), **electronic warfare**, **signal intelligence**, **computer security** (COMPUSEC), **command, control, communications, computers, and intelligence** (C4I), and **information operations** (IO) (also corresponds to DoDI 5230.29; consult your organizational security officer for possible COMPUSEC impact and TRADOC G-6 for possible COMSEC impact);
- Initial announcement of **GO assignments**;
- Initial announcement of awarded **Army contracts valued at more than \$3 million**, which will be made IAW the applicable provisions of the Federal Acquisition Regulation (FAR), the Defense Federal Acquisition Regulation Supplement (DFARS), and the Army Federal Acquisition Regulation Supplement (AFARS);
- Lists of names and / or duty addresses of military personnel assigned to **units that are sensitive, routinely deployed, or stationed in a foreign territory**;
- **Casualty information** on key U.S. government personnel or equivalent foreign-government personnel;
- Information on **activation, inactivation, or reorganization** of Active Army brigade or larger units; and
- Information on DoD **counterterrorist activities** as defined by DoD policy.

Official DoD information proposed for public release that meets any of the following criteria in DoDI 5230.29 must be **submitted to OSR for review and clearance if the information**:

- Affects national security policy, foreign relations, or ongoing negotiations;
- Is presented by a DoD employee, who, by virtue of rank, position or expertise, would be considered an official DoD spokesperson;
- Contains technical data, including data developed under contract or independently developed and subject to potential control that may be militarily critical and subject to limited distribution, but on which a distribution determination has not been made;
- Discusses and may affect the OPSEC of IEDs; or
- Discusses and may affect the OPSEC of initial fixed weapons basing and arms-control treaty implementation.

For more information, see AR 360-1 and DoDI 5230.29.

Organizational OPSEC officers should help ensure that any critical or sensitive information disapproved for release on the organization's Website is not approved for release into the public domain via any other venue, such as via official letters, resumes, articles for publication, email, official blog postings, discussion in Internet information forums, discussion in Internet message boards, or other forms of dissemination or documentation. IAW AR 530-1, **information not authorized for accessibility to the public on a Website is also not releasable in any other public forum**. This also **applies to Army homepages using a .com Internet service provider for official business**, since the Army charges the Army Web Risk Assessment Cell (AWRAC) to conduct OPSEC reviews and threat assessments of Army Websites not only on the .mil but also on all other domains used for communicating official information to ensure they are compliant with DoD and Army policies and best practices.²¹³

OPSEC review should only be accomplished by personnel who have **proper OPSEC certification**, such as the three-day HQ DA OPSEC officer course (Level II training). (If the organization has no qualified OPSEC officers, consult

²¹³ Paragraph 5-10, AR 25-1.

the TRADOC OPSEC officer for an alternate reviewer.) OPSEC reviewers must be expert in the rules governing FOUO information, as well as familiar enough with SCG to know what information must be referred to the organization's security manager for security review. OPSEC reviewers must also be familiar with the aspects of the organization's operations considered critical, its vulnerabilities, as well as the pertinent threat, so they can assess the nature of the risk associated with posting specific information to Websites.²¹⁴

If the **primary organizational OPSEC reviewer is also a content provider**, another organizational OPSEC officer – someone not involved with the production and / or dissemination of the particular piece of content being reviewed – should be the OPSEC reviewer.

The **OPSEC review must be done prior to the organization's submission of the information to Public Affairs** for approval of the information for public release. The office providing the information to PAO coordinates for the OPSEC review, and PAO is required to consider the evidence of that review in its assessment.²¹⁵

Before we move into the security manager's roles and responsibilities in reviewing Web content, we'll give two **real-world examples** of an OPSEC reviewer's tasks and responsibilities. The first example involves several photographs found in a February 2009 OPSEC review of HQ TRADOC's public-domain Web content. (Yes, we're telling on ourselves.) There were several mistakes in the review process of these photographs: they were not reviewed for OPSEC before a member of TRADOC PAO posted them on the HQ TRADOC Website, and they were probably ill-advisedly released by a CoE PAO in the first place. We'll show you two of these photos; we won't show the third one, which had Secure Internet Protocol Routed Network (SIPRNET) Internet Protocol (IP) addresses taped to the wall above the computer, as well as SIPRNET IP addresses on the computer screen.



Adversaries enlarge photographs to examine computer screens, as the case with these photographs, or background information (such as signs and charts on the wall), and thus glean information we really shouldn't make it so easy for them to get.

²¹⁴ Paragraph 3.5.2, Part II, DoD Web policy.

²¹⁵ Paragraphs 2-2c, 2-3a(14) and (15), 2-19 and 5-1, AR 530-1; Paragraph 3-3i, AR 25-2; Paragraph 5-4, AR 360-1.

An OPSEC reviewer should have examined these photographs before they were posted / released and enlarged the photographs to carefully examine them. The OPSEC reviewer should have recommended not releasing these photographs because they show diagnostic-check information on helicopters; the adversary can use these and the weapons-schematics used in training (and which show up on the public-domain Web) to assess where our weapons and systems are vulnerable.

The second real-world example involves the new initiative at the Basic Combat Training (BCT) CoE to establish and maintain new Websites and new Website concepts that are designed to increase communication between units and Soldiers' families during the initial-entry-training (IET) process. Although a dynamic idea, it also will involve balancing these communication attempts with continual OPSEC risk assessment. The initiative not only involves an enhanced family Website at the BCT CoE (see below) but also a Website established for families of future Soldiers at the URL of www.futuresoldiertrainingcenter.com.

As leaders believe it is important to connect new Soldiers' families to the Army because the level of family connection / integration impacts Soldier deployability, the new Websites will be "content-managed" Websites that "encourage active communication between unit leaders and Soldiers' family members. [The initiative] requires units to rethink Websites from one-way 'static brochures' to dynamic two-way communication mediums. These Websites may link with other communication systems such as Army virtual family-readiness groups and e-Army messaging."²¹⁶

One BCT CoE battalion's Website – 2nd Battalion, 39th Infantry – is already live at <http://www.jackson.army.mil/units/239/index.html>. Websites will feature galleries of photographs ("unlimited photos") taken and chosen for posting by the cadre; unit-leader blogging ("will open up communication with families"); on-line graduation ceremonies (so that family members who can't make the trip to see their Soldier graduate can still "participate" in the ceremony and look for their Soldier; these videos are to be updated for every BCT graduation ceremony); training videos (e.g., machine gun, bayonet, weapons, AT4, and M203 training); a document repository for family information; and information on the training unit's cadre (biographies and photos, although these individuals are not command spokespersons).

The primary issue with this initiative is, and will be, lack of OPSEC oversight and review before these items are posted; while the risk of posting individual pieces of information may be low, the opportunity for aggregation, as discussed in the section about PII earlier in this chapter, greatly increases the risk. In this type of situation, an OPSEC reviewer should conduct quarterly reviews and include the risk of aggregation in his / her assessment.

REVIEWER ROLES AND RESPONSIBILITIES: SECURITY MANAGER

Security reviewers review content IAW DoDD 5230.9, DoDI 5230.29, and AR 380-5. There are other types of information that require application of controls and protective measures for a variety of reasons²¹⁷ – this is CUI, IAW DoDD 5200.1-R; assessment for national-security information and CUI are separate programs, governed by separate regulations, and thus are separately reviewed in the Web-content-review process.

The organizational security reviewer's roles and responsibilities (some have already been outlined in the OPSEC-reviewer's section) are:

- Review proposed content for **classified** information as part of his / her role in ensuring that classified information is properly identified and protected;
- Assist the organizational OPSEC officer in determining if information would be **classified by compilation**;
- Assist the content provider or organizational OPSEC officer in identifying **national-security information** that must be sent to HQ DA and OSD for clearance, as listed in Paragraph 5-3, AR 360-1, and Enclosure 3, DoDI 5230.29, and provide a recommendation to PAO;
- Assist in identifying **unclassified information regarding classified programs**; and
- Assist the OPSEC reviewer with the pertinent **SCG(s)**.

Organizational OPSEC officers and security managers will consult TRADOC G-2, especially the FD officer, if proposed content could involve **Allied officers** based at HQ TRADOC or the centers / schools.

²¹⁶ According to Lt. Gen. Benjamin Freakley, commanding general of U.S. Army Accessions Command, at his March 13, 2009, presentation to spouses of TRADOC Senior Leaders Conference attendees.

²¹⁷ Paragraph 5-1a, AR 380-5.

G-2 also serves as a coordinating organization for establishing local procedures for Web review and clearance of information.²¹⁸ Also, in coordination with TRADOC PAO, TRADOC G-2 reviews proposed public releases on classified programs to preclude the release of classified information covered under the FOIA.²¹⁹

IAW DoD Web policy, when users of a Website believe that information, compiled or aggregated on a system or systems to which they have access, contains classified information, they may contact the Webmaster of the system(s) in question. Or, if the Webmaster is unknown, they may report the matter to their own organization's security officer for evaluation and action as appropriate.²²⁰ G-2 may advise organizations on the content in the event of this type of report.

Organizational security managers may use the OPSEC / security checklist at the end of this chapter to aid in their reviews.

REVIEWER ROLES AND RESPONSIBILITIES: SJA

SJA offices provide content review at HQ TRADOC, MSO, and CoE level by request from commands, units, or organizations before materials are posted on a public Website. Coordination and review may also be done for content to be posted on the AKO unrestricted-content area.²²¹

The SJA reviewer's **roles and responsibilities in reviewing content are:**

- Provide legal counsel if an organization proposes to release **FOUO information** is proposed to the public, IAW AR 530-1. (See the OPSEC reviewer's section, beginning on Page 49).
- Provide guidance on **copyrights and copyrighted material**. E.g.:
 - Advise organizations that copyrighted material may be used only when allowed by prevailing copyright laws, and only if the materials relate to TRADOC's mission.²²²

No copyrighted information may be posted without the **express written permission of the copyright owner**.²²³

Organizations wishing to post copyrighted information must consult legal counsel, and must provide a copy of legal counsel's opinion as part of the TRADOC content-review process. Organizations must also establish a procedure with the original content owner for **updating any information and for periodically verifying its releasability, currency, and accuracy**.²²⁴

- Advise organizations not to include **copyright notices on their Webpages**, as works by the U.S. government are not eligible for copyright protection.
- Advise organizations, when they wish to **republish news stories**, that they may provide a link to the story hosted on the source Website, with the appropriate external-links disclaimer, but that to republish the story on the TRADOC Website requires written approval from the news source.
- Advise organizations on **"fair use."**
- Advise organizations on use of **frames** on their Websites if there are copyright or trademark issues (see "content limitations" section in Chapter 4, Page 171).
- Ensure that organizational Websites do not engage in **conflicts of interest**. IAW the Joint Ethics Regulation (JER), conflicts of interest involve product endorsements or preferential treatment of any private organization or individual, which are prohibited on any official DoD publicly accessible site.²²⁵
- Advise organizations on the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002, or **No FEAR Act**, if they receive complaints about their Web content under the umbrella of this antidiscrimination and whistleblower-protection law. (The law requires each agency to post quarterly "No FEAR" **reports to their public Websites**; ensure ready access by both employees and the public; and provide links to the No FEAR Act reports from all major Web gateways. Organizations at ACOM-and-below level are not required to post No FEAR reports. The Army's most recently quarterly statistics will

²¹⁸ Paragraph 1-5i(3), TR 25-1.

²¹⁹ Paragraph 1-7m and Appendix F, AR 380-5.

²²⁰ Paragraph 3.5.4.2, Part II, DoD Web policy.

²²¹ Paragraph 2-3a(15), AR 530-1; Paragraph 6-7c(3), AR 25-1; Paragraph 6b(8), TRADOC OPSEC Plan.

²²² Paragraph 3.5.5, Part II, DoD Web policy.

²²³ Paragraph 2.3, Part II, DoD Web policy.

²²⁴ Ibid.

²²⁵ Paragraph 3.5.6, Part II, DoD Web policy.

be posted on the Army Review Board Agency's Website, <http://www.arba.army.pentagon.mil>, once this fiscal year's Annual Federal Equal Employment Opportunity Statistical Report of Discrimination Complaints (EEOC 462 Report) is complete.

- Review all completed **multimedia / VI productions** before they are posted to the publicly accessible Web (or distributed elsewhere, for that matter) to ensure that there are **no legal encumbrances** such as copyright, patent, personal property, or performance restrictions.²²⁶ Ensure that the organization has obtained all required releases.²²⁷ Ensure that any contractor(s) for the multimedia / VI product has assigned all interest in the work, to include copyright, to the government.

Before personnel, equipment, property, and so on are included in motion media, audio and video recordings, still imagery (e.g., drawings), electronic imagery, and other VI products, releases are required to use them and must be obtained **prior to their inclusion**. IAW AR 25-1, the **releases are required whether the product is for internal DoD use or release to the press, public, or individuals**. For policies governing these releases, legal counsel may refer to DoDI 5040.07, AR 25-55, AR 340-21, AR 380-5, DA PAM 25-91, and AR 360-1.²²⁸

SJA reviewers may use the legal counsel's checklist at the end of this chapter to assist in their Web-content reviews.

REVIEWER ROLES AND RESPONSIBILITIES: QI PROGRAM REVIEWERS

The QI review? Never heard of it, you say?

We'll explain, since technically, content not meeting QI standards should not be posted on TRADOC publicly accessible Websites, as QI is a federal law as well as DoD and Army policy.²²⁹ Each organization's content-review process must therefore include consideration of QI standards and elements.

The requirements and exceptions. Federal agencies, IAW the Information Quality Law²³⁰ and Paperwork Reduction Act (PRA),²³¹ are required to establish information-quality guidelines for the information they distribute. The QI program²³² focuses on the neutrality, usefulness, and integrity of information used and distributed by federal agencies. It also ensures that affected members of the public have an administrative mechanism to seek and obtain correction of information that does not meet quality standards.

²²⁶ Paragraphs 7-10b(4)k and 7-10b(4)l, AR 25-1. Per these references, the multimedia / VI product may not be cleared for release until the encumbrance has been removed.

²²⁷ Paragraph 7-10b(4)i, AR 25-1.

²²⁸ Paragraph 7-10b(4)k, AR 25-1.

²²⁹ Paragraph 1-12, AR 25-1. The federal law is discussed in the following footnote. DoD policy (via memo from the DEPSECDEF, "Ensuring the Quality of Information Disseminated to the Public by the Department of Defense," Feb. 10, 2003) requires DoD components to be ensure that disseminated information meets the standards of quality, objectivity, utility, and integrity, and to provide an administrative mechanism for affected persons to seek and obtain correction of information not complying with the standards. Army policy is stated in Paragraph 1-12b, AR 25-1: "Army organizations will establish standards of quality that are appropriate to the nature and timeliness of the information they disseminate. Organizations will not disseminate substantive information that does not meet a basic level of quality."

²³⁰ Paragraph 1-12a, AR 25-1, cites Section 3506, Title 44, USC, as the federal-law reference, but for clarity we'll state here that we're using Section 515, Treasury and General Government Appropriations Act for Fiscal Year 2001 (Public Law 106-554; H.R. 5658; the Federal Information Quality Act) and "Guidelines for Ensuring and Maximizing the Quality Objectivity, Utility, and Integrity of Information Disseminated by Federal Organizations" as the federal references. The Federal Information Quality Act, an often-overlooked law, directed OMB to issue government-wide policy and procedural guidelines to federal agencies for ensuring and maximizing the quality, objectivity, utility, and integrity of information (including statistical information) disseminated by federal agencies. All federal agencies were required, in turn, to publish QI guidelines; maintain the basic standards of information quality; and incorporate information-quality criteria into public information-dissemination practices. (OMB's guidance is outlined in more detail in the "general federal requirements" section of Chapter 4.) The Information Quality Law guidelines went into effect Oct. 1, 2002. OMB complied with the law's requirement in its memorandum, "Executive Branch Implementation of the Information Quality Law," Oct. 4, 2002, accessible at http://whitehouse.gov/omb/infoleg/pmc_graham_100402.pdf. The DEPSECDEF then issued the DoD policy memorandum referred to in the preceding footnote. The DEPSECDEF's guidance was adopted as Army guidance, IAW instruction in HQ DA Letter 25-03-02, "Ensuring Quality of Information Disseminated to the Public by the Department of Defense," Oct. 28, 2003. Although the HQ DA letter expired Oct. 28, 2005, and the QI Program has since been included in AR 25-1 and DA PAM 25-1-1, the DEPSECDEF and OMB memos have not expired.

²³¹ 44 USC, Chapter 35. More information on the federal Web standards is included in Chapter 4.

²³² Paragraph 1-12, AR 25-1; Paragraph 7-7a, DA PAM 25-1-1.

This **Guide** covers only the pre-dissemination requirements, as the post-dissemination redress avenues are established by other means.²³³ The Army's CIO / G-6 is the appeal authority to receive and resolve claims alleging that Army information disseminated to the public fails to comply with the QI standards. The Administrative Assistant to the Secretary of the Army (AASA) is another Army representative to receive and resolve QI claims.²³⁴ TRADOC G-6 serves as the liaison with Army G-6 to receive and resolve QI appeals.

The Army's QI Program is included in AR 25-1 and DA PAM 25-1-1. TRADOC does not have a formal QI program, so **Web-content QI reviewers provide pre-dissemination and post-dissemination content review by request from content providers or Website coordinators.** TRADOC PAO encourages QI review to be accomplished at organizational level to ensure adherence to quality standards; since QI *is* federal law, as TRADOC PAO completes our pre-dissemination reviews, we look for evidence that QI review has been performed as we make our determination whether or not to clear information intended for posting to the Web.

Specific reviewers are not required in most cases, except for scientific and technical information (more details on that follow), but TRADOC organizations must do a thorough copy-editing before submitting information to TRADOC PAO to check spelling, grammar, capitalization, syntax, errors in fact, and other content errors. Otherwise, organizations should avail themselves of TRADOC SMEs to review information to ensure accuracy, objectivity, and integrity. **By law, information products must undergo technical, supervisory, editorial, and legal review based on the product's nature.** QI reviewers may include an independent SME, statistical expert, IT expert, VI specialist, or an accessibility specialist.

Informal and formal reviews must ensure that products meet a minimum quality level. Organizations must treat information quality as an integral part to every step in the development of information, and therefore must allow adequate time for the QI review process, consistent with the standards required for the type of information being distributed. When appropriate, organizations must conduct QI reviews through the various stages of data development.²³⁵

Organizations are encouraged to incorporate procedures for meeting and maintaining QI standards into their existing information-resources management (IRM). For instance, integrity standards can be included in measures taken to implement the computer security provisions of the PRA. Website quality is covered by this **Guide**, which includes clearance procedures in the DoD Web policy, DoDD 5230.9, and other policies / guidance.²³⁶ However, since organizations must publish IRM procedures for reviewing and substantiating the quality standards of information before it is disseminated, adherence to procedures in this **Guide** will help serve as review and substantiation IAW DoD policy.²³⁷

Specific types of non-public content are exempt from the QI standards.²³⁸ The types of information (must be on non-public Websites) are:

- Distribution of information that is limited to government employees, Army contractors, or grantees.
- Intra- or inter-Army or other department / agency sharing of government information, including responses to requests under FOIA, the Privacy Act, the Federal Advisory Committee Act, or other similar laws.

There are several caveats on how to apply the DoD QI guidelines. They are:

- The QI guidelines apply to information that an organization disseminates from a publicly accessible Website or portal, but they do not include the hyperlinks to information others disseminate.

²³³ See Paragraph 7-7e, DA PAM 25-1-1.

²³⁴ Paragraphs 2-1s and 2-8h, AR 25-1.

²³⁵ Paragraph 7-7d, DA PAM 25-1-1.

²³⁶ Paragraph 3.1.1.3, Attachment 1, DEPSECDEF memorandum, "Ensuring Quality of Information Disseminated to the Public by the Department of Defense," Feb. 10, 2003.

²³⁷ Paragraph 3.2.1, Attachment 1, DEPSECDEF memorandum, "Ensuring Quality of Information Disseminated to the Public by the Department of Defense," Feb. 10, 2003. The QI requirement is in two parts, a means of review to ensure QI pre-dissemination, which is suggested by this **Guide**, and a means of redress for complaints, which is outside the scope of this **Guide**. Further, organizations must make public this means of redress, per Paragraph 3.3.1 of the DEPSECDEF memorandum. A memorandum from OMB, "Executive Branch Implementation of the Information Quality Law," Oct. 4, 2002, contains more in-depth information about handling "correction" complaints, as do Paragraphs 3.3.2 through 3.4.1 of the cited DEPSECDEF memo.

²³⁸ Paragraph 1-12c, AR 25-1; Paragraph 7-7c, DA PAM 25-1-1.

However, TRADOC's goal is that users of its public Website are assured access to accurate official information, "regardless of whether the site is linked only to other government Websites or also to private-sector Websites."²³⁹ QI reviewers must therefore evaluate links to private-sector Websites, to ensure the Websites meet QI standards, support the organization's mission, and are worthy of the link from an Army official Website.

- The QI guidelines also do not apply to opinions if the organization's presentation makes it clear that what is being offered is someone's opinion rather than fact or the organization's views, *unless* the organization represents the information as, or uses the information in support of, the organization's official position. Organizations should use disclaimers to distinguish the status of information they consider their own information holdings.²⁴⁰
- If the organization directed that information be prepared and / or disseminated by an outside party, such as a contractor, the organization retains the authority to approve the information before release. The organization is sponsoring dissemination of the information, making it subject to the DoD QI standards.²⁴¹

The standards. The TRADOC content-review process helps ensure QI, but there is also individual responsibility and accountability: content providers, organization Webmasters, content reviewers, and Website coordinators / Web-content managers must be diligent in monitoring posted information for timeliness, quality, objectivity, utility, and integrity. Content providers and reviewers should also carefully scrutinize their proposed content for QI standards.

There are three basic standards of information quality: objectivity, utility, and integrity. The term *quality* itself comprises objectivity, utility, and integrity of disseminated information to the general public. *Utility* refers to the usefulness of the information to intended users, including the general public – for instance, its availability to all persons IAW Section 508 of the Rehabilitation Act. *Objectivity* focuses on whether the information itself, as a matter of substance, is accurate, reliable, and unbiased, and on if its presentation is accurate, clear, complete, and unbiased. *Integrity* refers to security – the protection of information from unauthorized access or revision to ensure that the information is not compromised through corruption or falsification. The integrity of confidential information must be maintained, and confidential information must not be provided on the public Web.

DoD considers these standards "substantive terms."²⁴² (See the definitions section for more details on the QI standards.) Content providers and reviewers focus on the standards of *utility* and *objectivity*, while IA personnel focus on the standard of *integrity*.

One of the *utility* standards is that there are no abbreviations on an organization's homepage – abbreviations may be used on other pages if the words are spelled out first.²⁴³ Other QI standards mentioned in Chapter 2 were:

- Accurate spelling and punctuation;
- No factual errors or misleading information; and
- Written in understandable language, including for those with limited English proficiency.

Organizations wishing to publicly disseminate scientific and technical information must not only have an OPSEC / security review²⁴⁴ but must have an extra level of QI standards review: scientific and technical information is also subject to a formal, independent, external peer review. If scientific, financial, or statistical information is deemed to be "influential," there is a higher QI standard than peer review; the information must be capable of being "substantially reproduced" IAW commonly accepted scientific, financial or statistical standards.²⁴⁵ (Detailed Army guidance on implementing QI requirements can be found in Paragraph 7-7, DA PAM 25-1-1, and DoD guidance at <http://www.army.mil/CIOG6/references/policy/docs/U0167803.pdf>.)

²³⁹ Paragraph 8-1b, DA PAM 25-1-1.

²⁴⁰ Paragraph 3.2.4, Attachment 1, DEPSECDEF memorandum, "Ensuring Quality of Information Disseminated to the Public by the Department of Defense," Feb. 10, 2003.

²⁴¹ Paragraphs 3.2.5 and 3.2.6, Attachment 1, DEPSECDEF memorandum, "Ensuring Quality of Information Disseminated to the Public by the Department of Defense," Feb. 10, 2003.

²⁴² Paragraph 3.2.2, Attachment 1 (policy and procedural guidance), DEPSECDEF memorandum, "Ensuring Quality of Information Disseminated to the Public by the Department of Defense," Feb. 10, 2003.

²⁴³ Paragraph 8-2b(1), DA PAM 25-1-1.

²⁴⁴ See Paragraph 4b, DoDD 5230.9; Paragraph 4b, DoDI 5230.29; Paragraph 2-19, AR 530-1.

²⁴⁵ Paragraph 3.2.3.1, Attachment 1, DEPSECDEF memorandum, "Ensuring Quality of Information Disseminated to the Public by the Department of Defense," Feb. 10, 2003.

There are some caveats for PAOs regarding scientific and technical information. They are:

- PAOs do not have the authority to clear scientific and technical information for public release without prior review by SMEs, so the QI reviewer for scientific and technical information cannot be a Public Affairs professional. However, PAOs may assist the proponent of unclassified scientific and technical materials in determining at what level clearance can be granted. This material includes the results of RDT&E prepared for presentation or publication under AR 70-45, Paragraphs 5 and 7, within or outside the continental United States (CONUS). An exception is material that must be cleared through HQ DA or OSD IAW AR 360-1 and applicable industrial-security directives.
- Information jointly authored by Army and industry will be processed for review and clearance in the same way as materials of solely Army authorship.
- Scientific and technical information for public release will be prepared under AR 70-31. This material will be forwarded for clearance to the proper headquarters or administrative contracting officer.²⁴⁶

POCs. A QI POC is required²⁴⁷ in public Web content, so G-6 should appoint a QI officer, whose title and generic email address are to be included in public Web information. (The QI officer also performs any needed coordination with the QI designee at DA's FOIA and Privacy Act Division, Quality of Information Program.) HQ TRADOC organizations should appoint QI SMEs to accomplish QI reviews before the organization submits information to TRADOC PAO for approval to release publicly.

Organization Webmasters and content providers who receive complaints filed under QI guidelines, or IAW Public Law 106-554, should refer these complaints for resolution to the TRADOC G-6, monr.webmaster@monroe.army.mil.

The checklist at the end of this chapter may assist QI reviewers, as it prompts them to check areas discussed in this section.

In summary, before we move on to the final reviewer's (PAO's) roles and responsibilities, all organizational Webmasters, content providers, and content reviewers must ensure that Webpages meet the standards for quality, objectivity, utility, and integrity. All reviewers should conduct routine quarterly reviews of their organizational Websites in their areas of expertise to ensure that the Website is in compliance with DoD, Army, and TRADOC policy and guidance, and that content remains **relevant, appropriate, accurate, and current** – in short, the Website should provide reliable data in compliance with QI standards.²⁴⁸ Army policy requires the reviewer's minimum review to include all Website management control checklist items in Paragraph C-4, Appendix C, AR 25-1.²⁴⁹ Reviewers must keep written evidence of their reviews. (See Chapter 5 in this *Guide*.)

REVIEWER ROLES AND RESPONSIBILITIES: PAO

Public Affairs' content-review responsibilities are holistic and combine all items required for, as well as limited from, Web content in the publicly accessible domain. PAO reviewers review and approve for release any new content to be posted on their organization's corporate Website and to AKO unrestricted-content areas. New-content review will be conducted for 1) establishment of new Websites, 2) new Webpages or documents, and 3) major updates of Websites.

PAO reviewers should also conduct quarterly reviews of updated content after the content has been posted.

PAO's job, in addition to ensuring that all content proposed for release *is* releasable, is to ensure that all other reviews are done before clearing the information for posting in the public-domain Web. PAO reviewer responsibilities are varied and include:

- Establish local clearance procedures and **advise content providers at what level that review and clearance can be made**. Speeches and writings done in an official capacity must be cleared, but materials are cleared at the lowest possible level – preferably at the installation level. Local commanders have flexibility in releasing information.²⁵⁰

²⁴⁶ Paragraphs D-2a, D-2d, and D-2e, AR 360-1.

²⁴⁷ Paragraph 1-12b, AR 25-1; Paragraph 8-2f(1)(e), DA PAM 25-1-1.

²⁴⁸ Paragraph 6-7c(6)b, AR 25-1.

²⁴⁹ Paragraphs 6-7c(4) and 6-7c(6)b, AR 25-1; Paragraph 6b(8), TRADOC OPSEC Plan.

²⁵⁰ Paragraphs 5-3c(1), 5-3c(2), 6-6b, 6-7b, and 6-9a, AR 360-1.

- PAOs with subject-matter expertise and knowledge of the information's target audience can review and clear speeches and writings at the local level. But if material can't be cleared there, clearance will be completed at the next appropriate level.²⁵¹
- Whatever the clearance level, the approving PAO must revalidate the clearance before a content provider repetitively uses a previously cleared speech or writing.²⁵²
- If information lacks the proper clearance and has been sent by its author outside of TRADOC – for instance, to official Army publications – the publication's editor sends the information back to the proper clearance authority (PAO) at the lowest command level appropriate.²⁵³
- **Coordinate with OCPA on any information that must be submitted for clearance to HQ DA, OSD, or OSR.** OCPA manages the Army's Public Information Security Review Program, as well as the review-and-clearance process for information to be released outside DoD by the Office of the Secretary of the Army and the Army Staff.²⁵⁴
 - It is the author's / content provider's responsibility to ensure that content has been reviewed and cleared before public release.²⁵⁵
 - Official speech text and writings must be reviewed through Public Affairs channels and cleared for security, accuracy, policy, and propriety.²⁵⁶
- **Ensure that other reviews are completed as required.**
 - The OPSEC review is required, as a minimum, along with the PAO review. The staff office or agency providing the information to the PAO for release should accomplish the OPSEC reviews.²⁵⁷
 - Information proposed for posting on publicly accessible Websites must also be reviewed and approved by the information's proponent office before being released.²⁵⁸
 - Military-intelligence and security-related information, photographs, video, and audiotapes must be reviewed and authorized by U.S. Army Intelligence and Security Command (INSCOM).²⁵⁹
 - Releasing operational information on all Army Special Operations Forces (SOFs) must be coordinated with U.S. Army Special Operations Command (USASOC).²⁶⁰
 - When preparing material for release to the media on behalf of the commander, PAO coordinates for the security review, which can be done at the local level. Commanders below HQ DA level may release information wholly within their command's mission and scope if the information isn't restricted by the provisions of Paragraphs 5-3a and 5-3b, AR 360-1.²⁶¹
- **Review content** to be disseminated via the publicly accessible Web **before** the content is disseminated, as well as on a **quarterly basis after** information is disseminated via public Websites.
 - Releasable information must be accurate. Both the information and the organization's Website must comply with all applicable DoD and Army policies and guidance.²⁶²

What is reviewed. PAOs review all publicly accessible sites and conditions, which are defined as:

- An official Website posted on a .mil domain or other domain without access control;
- A Website using Secure Sockets Layer (SSL) restriction;
- A Website using a single password for all users;

²⁵¹ Paragraph 6-7b, AR 360-1.

²⁵² Paragraph 6-7n, AR 360-1.

²⁵³ Paragraph 6-9c, AR 360-1.

²⁵⁴ Paragraphs 2-2c(1), 2-2c(2), and 2-2c(3), AR 360-1.

²⁵⁵ Paragraph 6-1c, AR 360-1.

²⁵⁶ Paragraph 6-7b, AR 360-1.

²⁵⁷ Paragraph 5-4a, AR 360-1. Also alluded to in Paragraph 5-1c(1), AR 360-1: "Normally, such information is submitted to the appropriate PAO, who will ... ensure a security review is conducted."

²⁵⁸ Paragraph 6-6a, AR 360-1.

²⁵⁹ Paragraph 5-3c(5), AR 360-1.

²⁶⁰ Paragraph 5-3c(6), AR 360-1.

²⁶¹ Paragraph 5-3c(1), AR 360-1.

²⁶² Paragraph 5-4b, AR 360-1; Paragraphs 2-1g and 5-2d(3), AR 530-1.

- A Website that does not authenticate individual users;
- A Website that employs only domain or IP-address restriction as access restriction;
- A TRADOC AKO organizational portal that does not restrict access beyond basic AKO authentication;
- A File Transfer Protocol (FTP) site; or
- AKO unrestricted-content areas.

See the “public accessibility and Web security” section in the next chapter for more information.

What to review. Particular areas of review, at minimum, include:

- Compliance to Paragraph 6-7, AR 25-1, and Chapter 5, AR 360-1;
- That the organization’s content remains relevant and appropriate;
- That the organization follows the management-control checklist items of AR 25-1, Appendix C, Paragraph C-4;
- That the organization has the required links prescribed by DA PAM 25-1-1;
- That any organization lists are by title only, no personal names, unless there is an in-writing exception to the policy determined by the senior commander’s PAO IAW Paragraph 6-4r(1), AR 25-1;
- That there is no PII unless for designated command spokespersons (unless an OPSEC risk assessment clears it). PII will be treated as FOUO and operational information;
- That a keyword search has been done (and these sensitive documents removed) for deployment schedules; duty rosters; exercise plans; contingency plans; training schedules; inspection results, findings and deficiencies; non-command-spokesperson biographies; family-support activities; phone directories; lists of personnel.
- That there is no non-public information on the public Web, IAW Paragraph 1-7b, AR 25-1 (e.g., classified, restricted, or limited-distribution information; FOUO; unclassified information that requires special handling such as scientific / technical information protected under the Technology Transfer Laws; proprietary information; information that must be protected under legal conditions such as the Privacy Act; FOIA-exempt information);
- That secure Websites have effective passwords;
- That large directories of photographs be particularly reviewed for OPSEC violation in the aggregate and possibly secured in a private Website; and
- That there are no sponsorships or commercial advertisements, or any other sign of endorsement (such as a commercial logo), on official Websites.

PAOs may be assisted in their review tasks by two checklists at the end of this chapter: one for reviewing content for the Web and one for the releasability of information in general.

“Enduring” the content-review process is important, as providing information to key portions of the public and to the Army’s influential audiences is critical in maintaining public awareness and support for the Army.²⁶³ No matter how it seems to some, TRADOC’s review and clearance program isn’t a censorship activity. The program’s purpose is to safeguard writers / content providers and the Army – to prevent accidental release of inaccurate or inappropriate information, or even classified information. An added benefit is that the review process also helps PAOs stay abreast of their command’s public communications.²⁶⁴

TRADOC REVIEW STEPS

Now that we’ve talked about reviewer roles and responsibilities, we’ll move into how they are applied via TRADOC’s process. DoD has a prescribed information-posting process; the requirement is outlined in Paragraph 5.4.2, Part I, of the DoD Web policy, which requires leaders to ensure that all information is reviewed for “security, levels of sensitivity, and other concerns” before it is released on the publicly accessible Web – IAW the provisions of DoDD 5230.9 and DoDI 5230.29, and as described in Paragraph 3, Part II, of the DoD Web policy. Therefore this next section gets into the nitty-gritty, as it outlines procedures **TRADOC uses to integrate the requirements of**

²⁶³ Paragraph 6-1a, AR 360-1.

²⁶⁴ Paragraph 6-7c, AR 360-1.

DoD's information-posting process. (If you want a breakdown of Paragraph 3, Part II, of the DoD policy, plus DoDD 5230.9, and DoDI 5230.29, it's available in Appendix K.)

As encouraged by AR 360-1, the TRADOC Web Content Review Program keeps the approval process at the lowest possible level within the command. Thus the emphasis on reviewer roles and responsibilities, as the approval process begins within the organization providing the Web content and, as we've mentioned, Army policy requires pre-dissemination content review to be accomplished prior to information being posted.

The following are TRADOC's content-review steps when a content provider wishes to post information to the publicly accessible Web:

- (1) Organization commander / director oversight.
- (2) Organizational Webmaster for design coordination / consultation and verification / validation.
- (3) TRADOC Webmaster if the content will affect TRADOC's network.
- (4) OPSEC reviewer.
- (5) Security reviewer.
- (6) Army legal counsel / SJA designated representative, if needed / requested.
- (7) QI reviewer(s), as applicable.
- (8) PAO.

Commander / director oversight. The commander / director is key to a vital TRADOC Web Content Review Program, as he / she sets the conditions for success within his / her organization. Army regulations charge organizations to ensure the commander leads the review process for the WWW or AKO's unrestricted-content areas.²⁶⁵ **Commanders / directors are responsible for ensuring that their organizational Website complies with federal, DoD, and DA Website administration policies and with the implementing content-approval procedures that include OPSEC and PAO reviews before updating or posting information on all Websites.**²⁶⁶ Further, commanders / directors are responsible for ensuring that guidance is established that specifically assesses **data-aggregation concerns** and applies **risk-management strategies.**²⁶⁷ OPSEC and security are commander's programs; **commanders are tasked to conduct annual OPSEC reviews, which should include post-dissemination Web-content review of the organizational Website(s), and include these results in their annual OPSEC report IAW AR 530-1.**²⁶⁸ **Commanders / directors, or other Army public Website sponsors conduct an annual assessment of user satisfaction with their organization's Website, including usability, to identify needed improvements.**²⁶⁹ Because of these responsibilities, the organization's commander / director must be involved in his / her organization's Website content. Each Website must have a clearly defined purpose that supports the organization's mission, and the head of the organization, or his / her authorized representative, must **approve the defined purpose and general content of his / her organizational Website.**²⁷⁰ Steps 1 and 2 of Paragraph 3, Part II, DoD Web policy, are often initiated by the commander / director.

The commander / director – or his / her organizational OPSEC officer – is responsible for training his / her organization's personnel to understand that the value of information (and therefore the risk of its compromise or loss of access) may change in relation to the organization's objectives during peace, crisis, conflict, or post-conflict, as

²⁶⁵ Paragraphs 2-2 and 2-3, AR 530-1; Paragraph 6-7c(3), AR 25-1.

²⁶⁶ Paragraph 4-20g(11), AR 25-2. See also Paragraph 6a(6), Enclosure 2, DoD Manual 5205.02-M, which requires the head of the organization to further ensure **that compliance with content-approval procedures** for information intended for release outside the control of the organization, including release via a publicly accessible Website, **is evaluated during program reviews and other oversight activities** (such as inspections), and that the evaluation include assessment of the quality and effectiveness of integrating OPSEC into the organization's policies and procedures to identify and protect critical information. Refer also to Footnote 268, below.

²⁶⁷ Enclosure 2, Paragraph 6a(7), DoD Manual 5205.02-M; Paragraph 5-9, AR 25-1. AR 25-1 describes the four phases of a risk-management program, listing periodic review of the program as one phase.

²⁶⁸ Paragraphs 3-3i and 4-20g(15), AR 25-2. Web-content review is a force-protection and OPSEC measure; command OPSEC programs are examined as part of the TRADOC Command Inspection Program (CIP) – see Paragraph 5-4, AR 530-1. Paragraph 6a(9) in Enclosure 2, DoD Manual 5205.02-M, also requires that the organization's review program be evaluated during inspections, which should assess if education, training, and awareness are being conducted throughout the workforce. The customary annual period for the Army's OPSEC reporting is the fiscal year. According to the TRADOC OPSEC Officer (email dated Sept. 22, 2008), AR 530-1 requires that two points be addressed in the annual OPSEC report: 1) describe the procedures and protocols used to review open-source material for critical and sensitive information, and 2) describe the process to include OPSEC in the review of information prior to public release.

²⁶⁹ Paragraph 8-2g, DA PAM 25-1-1.

²⁷⁰ Paragraph 2.1, Part II, DoD Web policy.

well as during the various phases of an operation.²⁷¹ OPSEC and protection of information is a process that changes based on context – therefore the commander / director should emphasize to his / her content providers that they should habitually coordinate with the organization’s OPSEC officer.

The commander / director is also responsible for ensuring that his / her organization’s internal processes include a process for organization-wide review of staff documents to ensure protection of sensitive information. Organizations should adopt SOPs IAW AR 530-1 that state which documents (for example, news releases) automatically go to the organizational OPSEC officer and / or organizational security manager for review. (Documents that organizational OPSEC officers review include memorandums, letters, messages, briefings, contract, news releases, technical documents, proposals, plans, orders, responses to FOIA or Privacy Act requests, or other visual or electronic media.²⁷²) A good content-review SOP will clearly guide content providers and therefore should include references to DoD, Army, and TRADOC policy. The SOP should also provide standards for protecting, storing, and handling sensitive information. A good SOP should help prevent misunderstandings when content arrives in the PAO’s in-box for review and clearance approval. And a good SOP will guide the organization’s OPSEC officer in providing recommendations to the organization’s staff officers – often the organization’s Web-content providers.²⁷³

A note here because much of the TRADOC Web Content Review Program is accomplished internally in the organization providing the content. For instance, if not accomplished by the commander / director, Step 1 – and additionally Steps 2, 3, and 9 of the steps listed in Paragraph 3, Part II, of the DoD Web policy – are accomplished by the content provider or otherwise within the organization as part of the TRADOC content-review process. Step 4 is accomplished by the organizational OPSEC reviewer and organizational security reviewer; the content provider should assist. Steps 5, 7, and 8 are accomplished by the organizational Webmaster. Therefore it is vital that internal processes within the organization ensure an efficient, robust internal Web-content review process, and that these processes are established by the commander / director IAW Paragraph 3, Part II, DoD Web policy.

Organizational Webmaster. As mentioned earlier in this chapter, organizational Webmasters oversee design and network / bandwidth issues; perform analysis on Webpages for functionality and Section 508 compliance; verify hyperlinks as part of a QI review; determine access and security controls for content; and usually post their organization’s information. As part of the pre-dissemination review process, organizational Webmasters furnish evidence of their Section 508 testing for inclusion in the submission to PAO to clear proposed content for public release.

OPSEC reviewer. The organizational OPSEC officer also plays a key role, as he / she reviews content for OPSEC-sensitive information before it is submitted to Public Affairs for approval to publicly release the content.²⁷⁴ Evaluations of the organization’s Web content to be provided on the Non-Secure Internet Protocol Routed Network (NIPRNET) and publicly accessible Website(s) on the Internet must follow current OPSEC methodology.²⁷⁵ Possible risks must be judged and weighed against potential benefits prior to posting any Army information on the Internet.²⁷⁶

DoD OPSEC review requirements include:

- Formal review of content for its sensitivity (e.g., critical information, FOUO, or other CUI categories), sensitivity in the aggregate, determination of appropriate and / or intended audience, and distribution and release controls.
- Designation of individuals who have received the appropriate training in OPSEC, security, and release requirements to be responsible for reviewing information intended for public release, or inclusion of the OPSEC program manager / coordinator as part of the formal review process.
- Consideration of the method by which the information will be distributed, susceptibility of the information to data-mining, and the likelihood that the information could lead directly to the discovery and display of knowledge that is otherwise controlled. The ease with which data can be transferred to another media or distributed by another method should also be considered.

²⁷¹ Introduction, Chapter 1, Joint Publication 3-13.

²⁷² Paragraphs 5-1 and 5-2, AR 530-1.

²⁷³ Paragraph 3-57, FM 3-13.

²⁷⁴ Paragraphs 6a(1), Enclosure 2, and 3a(2)(d), Enclosure 3, DoD-M 5205.02; Paragraph 3-3i, AR 25-2.

²⁷⁵ Paragraph 1.3.4, Part V, DoD Web policy.

²⁷⁶ Paragraph 6-7c(3), AR 25-1.

- Requirement that release of information on DoD Websites and Web-based applications is IAW the **DoD Web policy**. Release officials must consider the **intended audience** and appropriate **Web domain** (e.g., publicly accessible, government-restricted, internal to the DoD component) and will restrict the information to that domain.²⁷⁷

Security reviewer. The security reviewer reviews proposed Web content IAW AR 380-5 and DoDD 5230.9, and the categories specified in Enclosure 3, DoDI 5230.29. Security reviewers assist organizational OPSEC reviewers in determining whether content contains any of these categories of prohibited information: classified, sensitive, critical, or CUI. The security reviewer also assists the OPSEC reviewer in determining if information is classified by compilation.

SJA reviewer. Legal counsel provides content review by request before materials are posted on a public Website. Areas of special interest include copyright and trademark, conflict-of-interest, selective benefit / endorsement issues, and counsel if organizations propose to post FOUO information to the public Web.

QI reviewers. QI reviewers review in their areas of expertise IAW federal law and DoD / Army regulation.

Public Affairs reviewers. Public Affairs reviewers ensure all reviews by all appropriate experts have been performed; **ensure the organization's story is told to the public**; and advise the content provider whether the organization's **corporate ethos** (e.g., the risk to the organization's credibility) will be impacted if publicly released information is omitted and / or deleted from the Web.²⁷⁸ At HQ TRADOC, release authority is the CPA or deputy CPA and cannot be further delegated; approval to post to the TRADOC Web must be received from either the CPA or deputy CPA. TRADOC PAO may further coordinate with OPSEC, security, or SJA reviewers, and with Section 508 and FOIA SMEs. The TRADOC Web Content Manager receives the submission and coordinates for its clearance from the CPA / deputy CPA and clarifies any issues with the submitter or other reviewer. PAO reviewers are responsible for consulting their command's / activity's OPSEC officer and security officer if questionable information is submitted, even if reviewed by lower-level organizational OPSEC reviewers. PAO reviewers consider the possible uses of the information, if released, by our adversaries because, after all, "[t]errorism has become a media event and, as such, a phenomenon of our time."²⁷⁹ PAOs should keep in mind that OPSEC and force protection override "general public affairs considerations."²⁸⁰

EXECUTION

There are several methods TRADOC PAO recommends that content providers may use to **send** their **files** to us through the process for review and approval. These methods are:

- For one file and up to a few files, email files as attachments to the reviewers. Using this method requires each recipient to save all the attachments within the proper directory structure before executing their browser and proceeding with the review. Email to TRADOC PAO content review, MONR-PAOContentReview@conus.army.mil.
- For a number of files or large files, create a compact disc (CD) and deliver the CD to TRADOC PAO. Content providers must ensure the CD is accompanied by a complete list of files to be reviewed.
- Place multiple, linking files – such as a new Website or major revisions to a section of an existing Website – on the TRADOC Web-development server and inform reviewers of their location (Web-development server URL). This method maintains the proper directory structure but incurs the risk of someone improperly viewing and / or posting the files before they are cleared / approved for release. Ensure the reviewer has access / permissions to the Web-development server.
- Alternately, make arrangements with the PAO reviewer for AKO access. Content providers may be provided their own restricted area on the WCWG portal, or they may provide access to the content provider's own AKO portal for the PAO and other content reviewers. Access to the WCWG portal is strictly controlled via a by-name listing in AKO. As long as the content provider's AKO portal is similarly

²⁷⁷ Enclosure 5, DoD-M 5205.02.

²⁷⁸ Paragraph 3.5.2.2, Part II, DoD Web policy.

²⁷⁹ Section 1 of Chapter II, Joint Publication 3-07.2.

²⁸⁰ See memorandum from the DEPSECDEF, "Information Vulnerability and the Worldwide Web," Sept. 24, 1998, and Paragraph E-1b, Appendix E, AR 380-5.

restricted, the risk is less than someone improperly viewing files posted on the Web-development server before the files are cleared / approved for release.

Emails should be used as the primary notification method that files are ready for the next step.²⁸¹

Content-review Steps 1 through 7 (listed in the previous section) are to be completed by the organization. Content providers should monitor accomplishment of the steps. These steps may be coordinated simultaneously, but Steps 4 and 5 should be coordinated closely together. Evidence of reviews / release, however, must be consolidated into one document provided to PAO. The consolidated document should provide names and contact information of all reviewers.

For each step in Steps 1-7, content providers will give each reviewer three working days to accomplish the review. Reviewers who need more time should coordinate with the content provider before the three days elapse to negotiate an extension.

For Step 8, a summary of all reviewer comments and the results of testing for Section 508 compliance must be forwarded to PAO. Public Affairs, as the release authority, is the final Web content reviewer. PAO reviews files and responds to the content provider via email with possible comments / revisions.

Since PAO as final content reviewer / approver may coordinate with any other reviewer in the process, PAO has five to seven working days to complete its review. PAO will consider requests for immediate review on a case-by-case basis, but these requests must be accompanied by a strong justification – lack of planning is not a justification.

After the content provider receives PAO's approval / clearance to post, and / or makes the requested changes, the next step is completed by the organizational Webmaster – once PAO release approval is received, documents are cleared for posting and do not need to be reviewed by anyone else.

When submitting materials for review / approval to PAO, content providers may use the checklist at the end of Chapter 2 to improve the coordination and review process.

POLICY VIOLATIONS

You've undoubtedly seen that the Web-content approval / posting process has built-in checks and balances. The process, at a minimum, involves an organization's leaders, its Webmasters / Website maintainers, its content providers, its content reviewers such as the OPSEC officer and QI expert(s), and its Web-content managers (Public Affairs). Each review / approval in the process helps identify policy compliance, QI, and security concerns before content is released publicly.

As stated, TRADOC's publicly accessible Webpages are a security vulnerability, as the enemy actively reviews DoD's public Web content,²⁸² and no pre-dissemination review process is foolproof. However, to comply with the SECDEF's direction that "[i]nformation is to be reviewed for data sensitivity prior to Web posting and protected

²⁸¹ Paragraph 6-1d, AR 360-1.

²⁸² DoD and Army leaders have repeatedly said this via policy directives and guidance memorandums. A sampling: "The enemy is highly adept at exploiting information vulnerabilities and actively searching for information on unclassified systems." – ALARACT message 089/2008, "Securing ACO Content and Credentials (NIPR)" (March 25, 2008). "Adversary intelligence collection threats include the exploitation of publicly available information often obtained through open networks and information on Websites." – Paragraph 4.3.1, DoDD 5205.2 (March 6, 2006). "The DoD Web-based data makes a vast, readily available source of information on DoD plans, programs, and activities. One must conclude our enemies access DoD Websites on a regular basis." – SECDEF message, "Website OPSEC Discrepancies" (Jan. 14, 2003). "The enemy aggressively 'reads' our open source and continues to exploit ... information for use against our forces. ... OPSEC violations needlessly place lives at risk and degrade the effectiveness of our operations." – ALARACT message 156/2005, "Chief of Staff of the Army OPSEC Guidance" (Aug. 23, 2005). "Recent events demonstrate that some Army personnel are disregarding good OPSEC discipline and are placing sensitive / classified information on the NIPRNET / Internet. ... The enemy has continuously shown an adaptive capability of gathering open-source information on Army operations, equipment and personnel." – ONTAP 04-01, "Security Classification Guidance (SCG) Extended for Operation Iraqi Freedom to Include Tactical Maneuver Plans and Operational Execution to Classification SECRET" (March 9, 2004). "Posting sensitive information onto public Websites allows our adversaries to obtain valuable information. ... In recent years, the Internet has become a greater source of open-source information for adversaries of the [United States]. Websites in particular, especially personal Websites of individual Soldiers (to include Weblogs), are a potentially significant vulnerability." – Paragraphs 3c and 4b(1)(b), TRADOC OPSEC Plan (July 10, 2006).

accordingly,”²⁸³ content providers must comply with the content-review process contained in this chapter to reduce risk.

Before we move into a short discussion of what happens when there’s a policy violation, it should be noted that not just OPSEC violations are policy violations. TRADOC Websites must also focus on providing value-added information services and products to the organization’s users, “customers,” the Army, and the general public by sharing accurate, timely, and relevant (“quality”) information²⁸⁴ via its general-public Website and its portal. As stated, QI is also DoD / Army policy and is required by federal law.²⁸⁵

This is important because, depending on the severity of the policy non-compliance, organizations in non-compliance may temporarily or permanently be revoked permission to post Webpages on the [army.mil](#) network. (Use of the Army NIPRNET to post organizational Websites is a privilege, not a right.) So that their organizations do not lose the WWW as a mission enhancement, TRADOC senior mission commanders should be vigilant about ensuring their public Webpages are free of major policy violations.

No publicly accessible official Website should link to an unofficial Website not in compliance with the JER and most DoD Web policy. Selecting and maintaining proper links from official sites to unofficial Websites is part of the checks-and-balances process. For instance, official links to unofficial Websites must comply with DoD, Army, and TRADOC policy for external links (consolidated in Chapter 4). Links to private official Websites must comply with policy and guidance for linking to sites with access controls.

Violation notifications. AWRAC, which is responsible for reviewing content of the Army’s publicly accessible Websites for ongoing OPSEC and threat assessment, identifies and reports Website violations. If AWRAC notifies an organization of a violation,²⁸⁶ the violation is usually severe or major / critical, and the violator is required to make immediate corrections or block the Website / link until the corrections are made.²⁸⁷ AWRAC’s remedial action required of the organization usually has a 24-hour suspense. (AWRAC’s notification will provide the details.) AWRAC checks all Army Websites – [army.mil](#) and other domains used for disseminating official information – to ensure they are compliant with DoD / Army policies and best practices.²⁸⁸

TRADOC G-6 and TRADOC PAO are also charged with post-dissemination content review and may use similar methods as AWRAC does (email notification and a violation-severity system) to assist content providers in achieving compliance to federal, DoD, Army, and TRADOC policy. Notifications from TRADOC PAO will be labeled severe / OPSEC, major / critical, or non-critical, similar to AWRAC’s methodology. The table on the following page provides the categories, response window, examples of what violations fall into the category, and notes for content providers and content reviewers.

If the violating page / site is not corrected within the prescribed time, the head of the POC’s organization and, if applicable, the Chief of Staff, will be notified. Notification will be made by either TRADOC PAO or TRADOC G-6, as coordination between TRADOC PAO and TRADOC G-6 will take place during the entire violation-notification process.

TRADOC G-6 and TRADOC PAO will coordinate with each other on all content-violation notifications. If either G-6 or PAO finds a possible OPSEC or security violation, they will immediately coordinate with an OPSEC or security SME (e.g., the TRADOC OPSEC officer in G-3/5/7 or the command security manager in G-2). If the SME determines the find is an OPSEC or security violation, the content reviewer will send immediate notification to the violator, courtesy copy-furnishing the TRADOC OPSEC officer and / or the command security manager as applicable.

At any time, if the situation warrants (such as a national-security violation), TRADOC PAO – as official spokesperson for the commander and content manager for the Web – or TRADOC G-6, as lead on TRADOC’s

²⁸³ SECDEF message, “Website OPSEC Discrepancies,” Jan. 14, 2003.

²⁸⁴ Memorandum from DISC4, “Guidance for Management of Publicly Accessible U.S. Army Websites,” Nov. 30, 1998.

²⁸⁵ Army public Websites must comply with applicable federal law, regs, and policies. See Paragraph 8-6a, DA PAM 25-1-1.

²⁸⁶ See Paragraph 4-20g(16), AR 25-2: “To verify compliance with federal, DoD, and DA Website administration policies, procedures, and best practices, AWRAC will continuously review the content of publicly accessible U.S. Army Websites to ensure compliance. ... AWRAC will provide results from these assessments to commanders for corrective actions.”

²⁸⁷ Paragraphs 5-10 and 6-7c(8), AR 25-1.

²⁸⁸ SecArmy’s executive-summary response to DEPSECDEF’s “DoD Website Security Policy Compliance” memo, Sept. 25, 2008.

Army Knowledge Management (AKM) and manager of Army networks, servers, and computer workstations – will access the Webserver and **unilaterally remove material**, with the TRADOC command group’s permission, without waiting for the process of violation correction to expire.

Category	Response window	Examples of violations	Other notes
Severe / OPSEC	Correct within 24 hours	Violations in this category will give away techniques, lessons learned, deficiencies, and vulnerabilities from recent and ongoing operations. An example of this type of violation is a large directory of photos which, in aggregation, should be defined as FOUO; any photo that shows details of Army equipment, including bumper / unit identification; or any photos of deploying Soldiers.	The most severe violation is a security violation. The violating content provides information of possible value to the enemy; it gives away critical information; it puts troops at risk; and it can be used by the enemy for targeting purposes. Most severe violations will be OPSEC violations. FOUO information such as this must be protected by PKI / CAC or other positive access control.
Major / critical	Correct within two working days if notified of the violation by TRADOC PAO; AWRAC's required response time from Website managers is normally 72 clock hours	These types of violations typically involve posting PII.	Following AWRAC's definition, a major / critical finding is “generally defined as information that in itself or in aggregation is or should be FOUO, or is typically FOUO as defined in Part V of the DoD Website Administration Policies and Procedures Guide.”
Non-critical	Correct within eight working days	These types of violations are non-compliance with DoD / Army regulation and policy, and may include advertising on an official site; non-compliance with required links in DA PAM 25-1-1; content that is not intended for the entire American public; content that is Section 508 non-compliant; or content that is out-of-date or inaccurate.	AWRAC concerns itself with OPSEC / security issues on public Websites, but there are non-OPSEC / security requirements that must be complied with. TRADOC G-6 and TRADOC PAO will monitor Websites for compliance with these requirements as well as for OPSEC / security concerns.

THE WCWG

The WCWG²⁸⁹ serves not only as a **forum to solve content issues** on the TRADOC Website but also as a **training and education venue**. The WCWG, as mentioned in Chapter 1, is part of the TRADOC Web Content Review Program. The WCWG should include:

- Each organization’s Website coordinator (see next chapter);
- QI SMEs; and
- SJA’s designated POC for Web-content issues.

The TRADOC OPSEC officer, FD officer, command security manager, and TRADOC Chief Knowledge Office (CKO) all tie in to the WCWG as SME consultants.

TRADOC WCWG personnel perform their work via the WCWG portal. The TRADOC WCWG also meets quarterly either in face-to-face meetings or via Adobe Connect (or similar method). In addition to the TRADOC WCWG, a WCWG should be organized at MSO / CoE level and convened at least quarterly. The senior commander’s PAO should chair the installation WCWG as the local overall Web-content manager; if the TRADOC

²⁸⁹ See TRADOC DCG / Chief of Staff memorandum, “TRADOC Public Website Content Management,” June 11, 2009.

senior commander's PAO is not the same individual as the senior commander's PAO, the TRADOC senior commander's PAO should represent TRADOC on the installation WCWG.

POST-DISSEMINATION REVIEWS

Most of the content-review efforts are concentrated in pre-dissemination reviews, but **post-dissemination content review must also be accomplished quarterly by all organizations**. TRADOC PAO and / or TRADOC G-6 will also review all organizations; organizations to be reviewed will include official, publicly accessible TRADOC entities on the WWW and AKO unrestricted-content areas.²⁹⁰ Organizations will be reviewed for compliance to policy, but particular areas of review, at minimum, will include:

- That the organization is in compliance with Paragraph 6-7c(4), AR 25-1, and Chapter 5, AR 360-1.
- That the organization's content remains relevant and appropriate.
- That the organization follows the management-control-checklist items of AR 25-1, Appendix C, Paragraph C-4.²⁹¹
- That the organization has the required links outlined in DA PAM 25-1-1.
- That any organization directories are by title only (no personal names), unless there is an in-writing exception to policy given by the PAO IAW AR 25-1, Paragraph 6-4r(1). The PAO's decision will consider OPSEC, including the possibility of sensitive information aggregated across Webpages, and will be determined in consultation with the organization's OPSEC officer.
- That there is no PII unless for designated command spokespersons or GOs / SESs, or unless PAO has granted an in-writing exception to a content provider's request for exception to policy. PII, which is FOUO, must be treated as operational information.²⁹² If the PAO has applied the "best judgment" standard, evidence of this deliberation will be provided to the quarterly content reviewer upon request.
- That a keyword search has been done (and these sensitive documents removed) for deployment schedules; duty rosters; exercise plans; contingency plans; training schedules; inspection results, findings, and deficiencies; non-command-spokesperson biographies; family-support activities; phone directories; or lists of personnel.²⁹³
- That there is no non-public information on the public Web, IAW AR 25-1, Paragraph 1-7b.²⁹⁴
- That secure Websites have effective passwords. The Webmaster as content reviewer should attempt to defeat the passwords (by using people's common mistakes with passwords) to help ensure that these Websites are non-publicly accessible.
- That large directories of photographs are reviewed for OPSEC violation in the aggregate and possibly secured in a private Website.

²⁹⁰ Paragraph 6-7c(3), AR 25-1.

²⁹¹ This checklist is formatted as "test questions" to which "no" answers constitute violations or possible violations. Test questions that apply to Web content are in Paragraph C-4e, Questions (25) through (34) (Appendix C in this **Guide**). This chapter also assists content reviewers with checklists for review.

²⁹² See the PII section, this chapter. Also, Paragraph C-4e, AR 25-1, uses the term "operational information" in Question (32).

²⁹³ Paragraph C-4e, AR 25-1, Question (34).

²⁹⁴ "Non-public" content includes PII / information prohibited from release by the Privacy Act; classified information; sensitive information; FOIA-exempt information (unclassified FOIA-exempt is also FOUO); or other categories as discussed at the beginning of this chapter. Non-public content may be shared for official purposes within the Army if the information is on an AKO KC (not the unrestricted-content areas) or other controlled-access (private) Webserver. Requests for non-public content must be coordinated with local FOIA / Privacy Act officials.

Webmaster Review Procedures Checklist				
Use this checklist in combination with the policy review checklist, following.				
Name of Reviewer		Date of Review		
URL of Webpage Reviewed		Organization Webmaster Name / Email Address / Phone Number (if different from the reviewer)		
Department / Organization Name		Content Provider Name / Email Address / Phone Number <u>OR</u> Website Coordinator Name / Email Address / Phone Number		
Issue / Concern	Yes	No	N/A	Notes / Comments
Pre-dissemination issues (for organizational Webmaster)				
Section 508 1a. Are all new and / or updated Webpages as well as all downloadable files (e.g., PowerPoint slides, PDF documents, and Microsoft Word documents) Section 508 compliant before they are posted, regardless of security controls in place? 1b. Has the organizational Webmaster performed Webpage testing for functionality and Section 508 compliance? 1c. Is a verification summary / results generation, or a justification on why the document does not have to meet Section 508 compliance, included in the submission request to PAO?				
2. Has the organizational Webmaster suggested an initial determination on appropriate access and security controls for content and coordinated with the organizational OPSEC officer on access and security controls?				See Paragraph 3, Part II, and Table 1, Part V, of DoD Web policy.
Quality of Information (QI) 3a. Has the organizational Webmaster verified that a QI review of the content has been accomplished within the organization? 3b. Has the organizational Webmaster validated all hyperlinks from the information before posting it as part of his / her own QI review?				IAW the "verification" step of Paragraph 3, Part II, of the DoD Web policy.
Metatags 4a. Has the organizational Webmaster obtained suggested metatags to include with each Webpage to assist with searchability of content? 4b. Has the Webmaster written the metatags into the page's code?				Certain metatags are required by Paragraph 8-3b(9), DA PAM 25-1-1, on homepages and major entry points: page title; description; creator / sponsor (in most cases, the organization's name); date created; and date reviewed. See Paragraph 5-3c, TR 25-1, for TRADOC's metatag requirements. Examples of how to write the metatags into HTML code follow this checklist.
5. Is the Webpage designed, developed, and tested for multiple browsers, operating systems, connection speeds, and screen resolutions, based on an analysis of an organization's Website visitors?				
Pre-dissemination issues (for HQ TRADOC Webmaster or TRADOC mission Webmaster)				

6. Has the overarching Webmaster been consulted if the proposed content will affect the Webserver / network?				
7. Is the page designed, developed, and tested for multiple browsers, operating systems, connection speeds, and screen resolutions, based on an analysis of an organization's Website visitors?				
8. Are all new and / or updated Webpages as well as all downloadable files (e.g., PowerPoint slides, PDF documents and Microsoft Word documents) Section 508 compliant before they are posted, regardless of security controls in place?				
Post-dissemination review (quarterly) (for all Webmasters)				
Violations 9a. Does the page / site comply with DoD Website administration policy, Army Website policy (AR 25-1), and Army information-resource management policy (DA PAM 25-1-1), TRADOC regulations, and guidance for official, publicly accessible Websites, and any subsequent policies and guidance memorandums? 9b. Have content providers been notified when there are "no" responses to Appendix C-4 test questions and other policy violations?				

The following gives examples of metatags in a Webpage's HTML coding. Information to be typed within quote marks is customized for each organization.

```
<HTML>
<HEAD>
<TITLE> </TITLE>
<META NAME="page title" CONTENT="Type the page title in here with organization name as the site's
sponsor">
<META NAME="keywords" CONTENT="Put keywords and phrases here, separate words and phrases with
commas, helps search engines">
<META NAME="description" CONTENT="This is where you put the description of the page's content">
<META NAME="sponsor" CONTENT="This is where you type in the creator or sponsor of the page or site">
<META NAME="date created" CONTENT="This is where you type in the date the page was created">
<META NAME="date reviewed" CONTENT="This is where you type in the date the page was last reviewed">
</HEAD>
<BODY> </BODY>
</HTML>
```

Policy Checklist for Army/TRADOC Websites				
IAW DoD and Army policy. See Paragraph C-4e, Appendix C, AR 25-1, for checklist of all key management controls as well as Paragraph 6-7, AR 25-1.				
This checklist is suggested for use by organization leaders, Webmasters, and Public Affairs officers to determine if Websites and Webpages meet DoD, Army, and TRADOC content policies, either pre- or post-dissemination of information; the completed checklist can also be sent to TRADOC PAO as a pre-dissemination approval / clearance tool when an organization is establishing a new Website or making major changes to an existing one.				
If the latter, send to TRADOC PAO's content-review email address, monr.contentreview@monroe.army.mil , or to TRADOC PAO's generic email address, tradocpao@monroe.army.mil . PAO reviewers review and approve for release any new content to be posted on an organization's corporate Website and to AKO areas accessible to all account types. PAO new-content review will be conducted for 1) establishments of new Websites, 2) new Webpages or documents, and for 3) major updates of Websites. PAO reviewers will also conduct quarterly reviews of updated content after the content has been posted.				
Name of Reviewer		Date of Review		
URL / Proposed URL		Organization Webmaster Name / Email Address / Phone Number		
Department / Organization Name		Content Provider Name / Email Address / Phone Number OR Organization's Website Coordinator Name / Email Address / Phone Number		
Target Date for Information to be Posted				
Check One: New Website [] Site Major Change [] New page [] Page Revision [] Summarize New Content or Changes Here:				
Issue / Concern (reviewer may wish to add comments in the blocks along with the issue / concern)	Yes	No	N/A	Policy Notes / Comments
Website purpose, organization mission, organization structure: 1a. Does the Website contain a clearly defined purpose statement that supports the organization's mission? 1b. Is the purpose statement backed by a Website plan that is approved by the organization's parent command or organization? Is the Website plan publicly available on the organization's Website?				AR 25-1, Paragraph C-4e, question (26). Each Website must have a clearly defined purpose statement and Website plan that supports the organization's mission. (See Paragraph 2.1, Part II, DoD Web policy, and Paragraph 8-1c, DA PAM 25-1-1.) The Website plan is to be documented (see Paragraph 8-1c(4), DA PAM 25-1-1) along with the organization's continuity-of-operations plan (COOP), which must comply with Paragraph 6-1b, AR 25-1. Organizations must consult SMEs as to the markings on their Website purpose statements and plans, as they may require FOUO marking; if so, revisions will be needed for a version to be posted in the public domain.
1c. Does the publicly available Website plan address the Website's registration?				See Paragraphs 8-1c(1) and 8-1e, DA PAM 25-1-1; and Paragraph 6-7, AR 25-1.

1d. Does the publicly available Website plan address Webmaster / portal administrator contact information?				At minimum, this must include the Webmaster's / portal administrator's generic email address for users to request information or to direct questions, comments or suggestions for that organization, IAW Paragraph 5-5b(3), TR 25-1. Organizations will use organizational designation / title and generic position email addresses, such as office@organization.mil , IAW ASD-C3I memorandum, "Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites," Dec. 28, 2001, and TRADOC Command Guidance: Noble Eagle #02-019, "Personal Data on Unclassified Websites," March 13, 2002.
1e. Is the contact information generic rather than by-name?				
1f. Does the publicly available Website plan address procedures that explain posting of information and review of the site for content and format?				See Paragraph 8-1c(3), DA PAM 25-1-1.
1g. Does the publicly available Website plan address contingency and continuity of operations, describing what the organization will do with its Website during disasters or emergencies, and what important information and services will be provided to the public?				See Paragraph 5-5b(3), TR 25-1; Paragraph 8-1c(4), DA PAM 25-1-1; and Paragraph 6-1b, AR 25-1.
2a. Does the Website include from its homepage a description (or a link to the description from the homepage) of the organization's mission and the organization's structure?				See Paragraph 5-5b(2), TR 25-1, and Paragraph 8-2f(2), DA PAM 25-1-1. Names of personnel in an organization chart or section chart becomes a list of personnel names, which is prohibited.
2b. Does this description exclude names of personnel?				
2c. Does the organization structural description avoid including FOUO information?				
Required notices:				AR 25-1, Paragraph C-4e, question (27). A WIS is a major division of content on a domain. Each WIS must contain on its first page / homepage the text, or a link to the text, of an approved privacy policy. DA PAM 25-1-1 also requires the privacy notice to be contained within the content of the "Important Notices" page. IAW Paragraph 6, Part II, DoD Web policy, all publicly accessible Websites must have both a "human readable" privacy policy and machine-readable technology that automatically alerts users about whether site privacy practices match their personal privacy preferences.
3a. Are users of each publicly accessible Website provided with a privacy and security notice prominently displayed or announced on at least the first page of all major sections of each Web information service (WIS)?				
3b. Does the privacy policy describe how, in general, security is maintained on the site, what specific information is collected, why it is collected, and how it is used? (All information collected must be described in this policy.)				
3c. Is the link to the "human readable" version of the privacy policy labeled "Privacy policy"?				
3d. Does the privacy notice or link to the privacy notice avoid the perception of danger (i.e., skull-and-crossbones logos or "warning" graphics)?				
3e. Does the privacy/security notice follow the recommended wording of the DoD Webmaster policy, or, if not, has it been approved by legal counsel and reviewed for OPSEC indicators and sensitive information?				
4a. If external links are present, does the Website contain a "disclaimer for external links" notice or intermediate "exit notice" page when a user clicks on a link to any unofficial Website?				AR 25-1, Paragraph C-4e, question (28). An external link is a link to any site outside the official DoD WIS – usually, but not restricted to, the .mil domain. The external-links disclaimer must be displayed when an organization links to an unofficial, "external" Website. The disclaimer must appear on the page / pages listing external links or through an
4b. Is the disclaimer IAW Paragraph 7.2, Part II, DoD Web policy, and Paragraph 6-7c, AR 25-1?: "The appearance of external hyperlinks does not constitute endorsement by the U.S. Army of this Website or the information, products, or services contained therein. For other than authorized activities such as military exchanges and MWR sites, the U.S. Army does not exercise any				

editorial control over the information you may find at these locations. Such links are provided consistent with the stated purpose of this Website."				intermediate "exit notice" page generated by the server. This standard applies to links from an official DoD site to any site other than an official DoD Website, IAW Paragraphs 7.1.6, 7.1.7, and 7.2, Part II, DoD Web policy, and Paragraph 6-7c, AR 25-1.
5. Has the organization included a hyperlinks policy / notice?				If organizations use external links, they must 1) establish objective and supportable criteria or guidelines for how they select and maintain their links to non-Army Websites, and they must 2) post these criteria, along with an explanation of their process for linking to these sites, on their publicly accessible Website. Organizations' linking procedures must explain why some links are chosen and others are not. The links must be chosen fairly and in the best interest of the public. (See Paragraph 8-1k, DA PAM 25-1-1, and Paragraph 6-7c, AR 25-1.) External-links guidelines must consider the information needs of personnel and their families, mission-related needs, and public-communications and community-relations objectives.
6a. If session cookies are used on this Website to collect personally identifiable information (PII) about Web visitors, is there a Privacy Advisory (PA) or Privacy Act Statement (PAS)? 6b. Is the Website free of persistent cookies or other devices designed to collect PII about Web visitors?				See Paragraph 11.2, Part II, DoD Web policy. Persistent cookies are prohibited on Army Websites unless the conditions of the DoD Web policy are met, including Secretary of Defense approval. AR 25-1, Paragraph C-4e, question (30).
7. Does the Website have a classification banner as the first page visitors come to?				Unclassified Webpages must be "marked" as to their classification. Each organization's unclassified Website homepage must include a banner stating that the Website contains only unclassified, non-sensitive, and non-Privacy Act information – Army policy requires this as the first page visitors come to. A banner similar to the one given in Figure E-1, AR 380-5, will be used; no further markings are required, IAW Paragraph E-6, AR 380-5.
Endorsement: 8. Is the Website free of commercial sponsorship and advertising?				AR 25-1, Paragraph C-4e, question (29). Official Websites are prohibited from displaying sponsorships or commercial advertisements, IAW Paragraph 9, Part II, DoD Web policy. See also DoDI 8410.01: "Websites and other Internet media in domains specifically funded by, registered to, or exclusively used by the Department of Defense, and visible to or distributed to the public, shall not be used to advertise or market private individuals, commercial firms, corporations, or not-for-profit firms. Such media must not imply in any manner that the Department of Defense endorses or favors any specific commercial or not-for-profit product, commodity, or service." Advertising implies

				endorsement, which is prohibited by Paragraph 3-209 of the JER: “Endorsement of a non-federal entity, event, product, service, or enterprise may be neither stated nor implied by DoD or DoD employees in their official capacities.”
Section 508: 9a. Is each Website made accessible to handicapped users IAW with Section 508 of the Rehabilitation Act? I.e.: 9b. Do videos include transcripts or captioning for the hearing impaired? 9c. Does audio include transcripts for the hearing impaired? 9d. Are pages designed for easy reading by screen readers for the visually impaired? 9e. Do photographs and other imagery have ALT tags? 9f. Does imagery such as icons aid understanding for the cognitive impaired? 9g. Do Webpages avoid requiring a high level of manual dexterity, such as complicated drop-down menus? 9h. Are all downloadable files (e.g., PowerPoint slides, PDF documents and Microsoft Word documents) Section 508 compliant? (See Appendix N for the accessibility standards.) 9i. Do PowerPoint presentations that contain graphics have an equivalent accessible file in text, HTML, or PDF?				AR 25-1, Paragraph C-4e, question (31). IAW Paragraph 6-7, AR 25-1, Army Websites must be accessible to handicapped users IAW Section 508 of the Rehabilitation Act. Transcripts for videos, or captioning for the hearing impaired, are required IAW Paragraph 7-7a, AR 25-1. Other Section 508 compliance requirements are listed in detail in DA PAM 25-1-1. All Army Websites must provide a link to the organization's accessibility policy from the “Important Notices” page (see Paragraph 8-3b(2), DA PAM 25-1-1).
Other accessibility / usability 10a. Has information been presented using plain language that considers the knowledge and literacy level of the typical Website visitor? 10b. Are the “height” and “width” attributes used as additions to the basic image-source tag? 10c. Do all button-type navigation graphics have height and width attributes?				See OMB memorandum M-05-04, “Policies for Federal Agency Public Websites,” Dec. 17, 2004.
Required Webpages: 11a. Does the Website include an “Important Notices” page? 11b. Is it linked from the footer of every Webpage in the site, as well as being accessible from the Website's homepage?				A link to the “Important Notices” page must be placed at the footer of every Webpage as well as being clearly accessible from the homepage. The “Important Notices” page describes principle policies and other important notices that govern the Website, especially those mandated by law. At a minimum, this page includes the requirements in 11c through 11f. (See Paragraph 8-2f(2)(k), DA PAM 25-1-1.)
11c. Does the “Important Notices” page include the organization's privacy policy, including its cookie policy?				The cookie policy must state that the Website does not use “persistent” cookies or any other automated means to track the activity of users over time and across Websites. The privacy policy must state how security is maintained on the site, what specific PII is collected, why it is collected, and how it is used. All information collected must be described in this notice. (See Paragraph 6, Part II, DoD Web policy.)

				See the DoD standard notice for the text.
11d. Does the "Important Notices" page include information on how Website visitors may request information under the Freedom of Information Act (FOIA)?				Website visitors must be advised how to make FOIA requests. FOIA requests are made to one central email: FOIA@mda.belvoir.army.mil .
11e. Does the "Important Notices" page include the organization's accessibility (Section 508) policy?				<p>The Section 508 policy must be posted on this page or be linked from it. Text will advise Website visitors that it is the Army's policy that its Websites are accessible to handicapped users IAW Section 508 of the Rehabilitation Act; describe the site's compliance with Section 508; and inform visitors whom to contact for a Section 508 complaint. (See Paragraph 8-3, DA PAM 25-1-1.)</p> <p>When the Website includes electronic forms meant to be completed on-line, a form must also be offered to allow people using assistive technology to access the information, field elements and functionality required for completion and submission of the form, including all directions and cues.</p>
11f. Does the "Important Notices" page include the organization's Quality of Information (QI) guidelines?				The QI policy will advise Website visitors, at minimum, that the organization's goal for its on-line information is accuracy, objectivity, and integrity, and that it undergoes technical, supervisory, editorial, or legal review as appropriate, based on the information's nature. Website visitors will also be given the generic contact information for the organization's information-quality POC.
12a. Does the Website contain a Webpage, or link to a Webpage, labeled "Contact Us" or "Contact [organization name]"?				Each Website must post a "Contact Us" page and provide links to it from the homepage and every major point of entry on the Website, IAW Paragraph 8-2f, DA PAM 25-1-1. The page must be labeled "Contact Us" or "Contact [organization name]" and contact information will be generic. Army policy (see Paragraph 8-2f, DA PAM 25-1-1) requires the specific items of content in 12d through 12j to be provided on the "Contact Us" page.
12b. Is the "Contact Us" page linked from the organization's homepage and every major point of entry?				See Paragraph 8-2f, DA PAM 25-1-1.
12c. Is the contact information provided generic in nature, rather than providing PII?				
12d. Does the contact Webpage include the organization's street address, including addresses for any regional or local offices?				
12e. Does the contact Webpage include office phone number(s), including numbers for any regional or local offices?				
12f. Does the contact Webpage include a means to communicate via email (organizational email address or Web-based contact				The means to communicate via email will not be a by-name email address. If a Web-based contact form is employed, if

form)?				PII is gathered, either a PAS or PA is required. See Paragraph 11.2, Part II, DoD Web policy.
12g. Does the contact Webpage outline the organization's policy and procedures for responding to email inquiries, including whether the organization will answer inquiries and the expected response time?				
12h. Does the contact Webpage contain contact information for the organization's QI Program POC?				
12i. Does the contact Webpage contain contact information (office names / titles / phone numbers) for small business to direct queries to?				Contact information (title / phone number) for small businesses is required by the Paperwork Reduction Act.
12j. Does the contact Webpage contain contact information for FOIA requests?				The means to request information through FOIA is also included on the "Important Notices" page. Instruct Website visitors on this page, too, to make FOIA requests by emailing FOIA@rmda.belvoir.army.mil .
13a. Does the Website contain a Webpage labeled "About Us" or "About [organization name]"?				If the site is a main-entry-point Website, such as an organizational homepage, it must contain a Webpage labeled "About Us" or "About [organization name]." Paragraph 8-2f(2), DA PAM 25-1-1, requires the specific items of content detailed in this checklist's questions 13c through 13l on the "About Us" page.
13b. Or, does the Website contain a link to TRADOC's "About Us" page?				
13c. Does the "About Us" page include a description of the organization's mission, including its statutory authority?				
13d. Does the "About Us" page include the organization's strategic plan (unclassified, sanitized version), vision, or set of principles?				
13e. Does the "About Us" page include the organization's structure, including basic information about the organization's parent and / or subsidiary organizations and regional / field offices?				
13f. Does the "About Us" page include contact information, which may include generic email addresses, office phone number, office name, or an individual's title (no by-name email addresses or personal names)?				
13g. Does the "About Us" page include information about professional opportunities / jobs at the organization?				Preference is to link to CPO on-line at http://acpol.army.mil/employment/index.htm . The site can also link to USAjobs.gov .
13h. Does the "About Us" page contain a link to a sitemap or subject index for the Website?				
13i. Does the "About Us" page contain a link to a "common questions" / FAQ page?				
13j. Does the "About Us" page contain easy access to existing on-line citizen services and forms?				The organization's Website must contain easy access to any on-line citizen services and forms it makes available to the general public, and this access (link) must be displayed as prominently as

				possible. Access to on-line services and forms must also be linked from the "About Us" page.
13k. Does the "About Us" page contain a link to a portal for the organization's most frequently requested publications?				Each Website must organize its most frequently requested publications into a portal. The "About Us" page must contain a link to the publications portal. (However, do not duplicate content on the HQ TRADOC homepage or Army Publishing Directorate Website.)
13l. Does the "About Us" page contain a link to the "Important Notices" page?				
14a. Does the Website contain a sitemap or subject index that gives an overview of the site's major content categories?				Each Website must include a site map or subject index that gives an overview of the Website's major content categories. At minimum, the sitemap must be linked from the homepage, IAW Paragraph 8-2f(2)(f), DA PAM 25-1-1.
14b. Is the sitemap or subject index linked to from the Website's homepage and its "About Us" page?				
15a. Does the Website contain a "common questions" / FAQ page that provides basic answers to questions the organization receives most often?				IAW Paragraph 8-2f(2)(g), DA PAM 25-1-1.
15b. Is the "common questions" / FAQ page linked to from the Website's homepage and its "About Us" page?				
16. Does the Website include a "Help" page that outlines major proposed and implemented changes to the Website?				IAW Paragraph 8-3b(10), DA PAM 25-1-1.
17. Does each page of the Website include either a search box or a link to a search page entitled "Search"?				Organizations must include either a search box or a link to a search page from every page of the Website. The search box or link will be entitled "Search." Webmasters will place subject and keywords in source code to aid content searches. Focused searches may be given to search within sets of information, databases or applications. Websites that are narrow in scope or less than 200 pages may substitute a sitemap or A-to-Z index rather than implement a search engine. (See Paragraph 8-3b(8), DA PAM 25-1-1. The paragraph also outlines minimum service-level standards for the search function.)
Required statements or other text:				
18a. Has a currency declaration on every Webpage (i.e., "Last updated on ____") or a date stamp been included on each page to indicate when last altered or reviewed?				<p>A currency declaration is required on every Webpage: "Army public Websites will clearly state the date the content was posted or updated for every Webpage indicating to visitors that the content is current and reliable." Webmasters must include a statement such as "Last updated on ____" or a date stamp on each page to indicate when last altered or reviewed, IAW Paragraph 8-11, DA PAM 25-1-1.</p> <p>The author of / POC for a publicly accessible Webpage should give generic email address contact information or a generic "mailto:" link (such as monr.webmaster@monroe.army.mil) for</p>

				Website visitors to contact if they find content to be incorrect or outdated.
18b. Does each Webpage state the organization's official name and display the phrase "This is an official U.S. Army site"?				Each Webpage must state the organization's official name and display the phrase "This is an official U.S. Army site." Homepages and second-tier pages must also include the organization's name identified as the site sponsor as part of the page title, IAW Paragraph 8-1i, DA PAM 25-1-1, and Paragraph 5-5b(5), TR 25-1.
18c. Do homepages and second-tier pages also include the organization's name identified as the site sponsor as part of the page title?				
19. Has a redirect notice / page been provided when links have been changed?				When Webpages are deleted, the Webmaster must 1) delete links from pages containing links to the page being deleted; 2) delete any associated files such as Word documents or images from the Webserver; and 3) use a redirect notice / page to provide Website visitors with substitute links or content when page destinations are changed by deleted Webpages.
Required links (required by Army and TRADOC policy): 20a. Does the homepage link to USA.gov , if applicable?				Major organizational pages must link to USA.gov from their homepage. The entry for the link shall read "USA.gov: U.S. Government Web Portal," IAW Paragraph 8-5d, DA PAM 25-1-1. Unless the organization is Army, Army-command or HQDA-staff-element level, a link to USA.gov is not required.
20b. Does the entry for the link read "USA.gov: U.S. Government Web Portal"?				
21. Is a link to the FAQ page provided from the "About Us" page?				IAW Paragraph 8-2f(2)(g), DA PAM 25-1-1.
22. Is a link to the portal for most frequently requested publication(s) provided from the "About Us" page?				IAW Paragraph 8-2f(2)(j), DA PAM 25-1-1.
23. Is there a link to the "Important Notices" page at the footer of every Webpage?				IAW Paragraph 8-2f(2)(k), DA PAM 25-1-1.
24. Is a link from the homepage provided to the "Help" page?				IAW Paragraph 8-3b(10), DA PAM 25-1-1.
25. Is there a link from the homepage to the sitemap or subject index page?				IAW Paragraph 8-2f(2)(f), DA PAM 25-1-1.
26. Is there a link from the homepage (at minimum; can be elsewhere through the site) to the next senior Website in the hierarchy?				All TRADOC sites must link to: the next senior Website in the hierarchy IAW TR 10-5; the organizational homepage on AKO if one exists; the TRADOC logo and motto; the HQ TRADOC homepage; and the Army homepage, IAW Paragraph 5-5b(1), TR 25-1.
27. Is there a link from the homepage (at minimum) to the organizational homepage on AKO if one exists?				Since the organizational homepage is access-controlled, there must be the appropriate disclaimer on the public site, near the link to AKO, per DoD Web policy.
28. Is there a link from the homepage (at minimum) to the TRADOC logo and motto?				IAW Paragraph 5-5b(1), TR 25-1.

29. Is there a link from the homepage (at minimum) to the HQ TRADOC homepage?				IAW Paragraph 5-5b(1), TR 25-1.
30. Is there a link from the homepage (at minimum) to the Army homepage?				IAW Paragraph 5-5b(1), TR 25-1.
31. Is there a link from the homepage to the organization's portal for its most frequently requested publications?				IAW Paragraph 8-2f(2)(j), DA PAM 25-1-1.
32. Do links to documents requiring downloading provide enough contextual information that visitors have a reasonable understanding of what to expect when they view the material after downloading?				IAW Paragraph 8-3b(5), DA PAM 25-1-1.
33. Does each Webpage link back to the Website's homepage and to its parent organization's homepage?				To improve Website utility, each Webpage must link back to the Website's homepage and to its parent organization's homepage, IAW Paragraph 8-5c, DA PAM 25-1-1.
34. If an organization uses a graphical link, does that link also contain text indicating that it links back to the homepage?				IAW Paragraph 8-5c, DA PAM 25-1-1.
35. Are links current and accurate?				
36. Do external links avoid requiring or encouraging users to choose any browser-specific software?				
37. Do listings of Web links separate external Web links from government and military links?				Paragraph 6-7c(7)(b), AR 25-1.
38. Do official Websites avoid linking to an unofficial Website not in compliance with Web policy?				
Standard navigation: 39a. If the organization is exempt from using TRADOC G-6's Webpage template, has consistent navigation between and within pages been established? 39b. Does CoE / mission Webpages' design make them distinguishable from garrison or other installation tenant activities?				Standard navigation criteria is contained in Paragraph 8-3b(7), DA PAM 25-1-1: <ul style="list-style-type: none"> • Common items among most Webpages must be in the same location on each page and have the same appearance and wording. • Navigation items of the same type will look and behave like each other. • If a set of Webpages requires specialized navigation, that navigation is applied to the largest possible local grouping and will be similar in appearance and behavior to the overall navigation scheme.
40. Have the most frequently requested publications been placed in a portal?				
41. Does the text placed in the <TITLE> and <H1> </H1> tags describe the information provided on that page?				
Proprietary tags and formats 42a. Have proprietary HTML tags such as <animate> been avoided? 42b. Have proprietary formats been used only when the audience is known to have easy access to software able to read the format?				
43. Have horizontal rules been used one at a time and only to				

logically divide unrelated sections of a single page?				
File management				
44a. Have unlinked Webpages been deleted from the live Webserver?				
44b. Has working-draft content been deleted from publicly accessible files or portals?				
45. Is FOUO information or information sensitive by aggregation posted to a Website that, at a minimum, uses Secure Sockets Layer (SSL) for transmission control and Public Key Infrastructure (PKI) at the software or hardware level for access control?				

OPSEC / Security Review Checklist				
<p>IAW Appendix C-4e, AR 25-1, and AR 530-1. The key-management-controls checklist in Appendix C of AR 25-1 is mandated by AR 25-1 as the minimum review. The following checklist is more in-depth and tailored to OPSEC and security reviewers. (However, there is no DoD or Army mandate for following this list; it is provided as a reviewer's aid.) Suggested use is for either pre- or post-dissemination content reviews.</p> <p>The OPSEC / security reviewer should screen for not just OPSEC indicators but for critical information, sensitive information, controlled unclassified information (CUI), For Official Use Only (FOUO) information, national-security information, and personally identifying information (PII).</p>				
Name of Reviewer		Date of Review		
URL / Proposed URL		Organization Webmaster Name / Email Address / Phone Number		
Department / Organization Name		Content Provider Name / Email Address / Phone Number <u>OR</u> Organization Website Coordinator Name / Email Address / Phone Number		
Issue / Concern (reviewer may wish to add comments in the blocks along with the issue / concern)	Yes	No	N/A	Policy Notes / Comments
Website purpose, organization mission, organization structure: 1a. Does the Website contain a clearly defined purpose statement that supports the organization's mission? 1b. Has this purpose statement been reviewed for OPSEC indicators and sensitive information? 1c. Is the purpose statement linked with a Website plan that is publicly available on the organization's Website? 1d. Has the Website plan that is/will be posted on the organization's Website been reviewed for OPSEC indicators and sensitive information? 1e. Does the Website include its mission statement? 1f. Has the mission statement been reviewed for OPSEC indicators and sensitive information? 1g. Does the Website include an outline of the organization's structure? 1h. Does the organization structural description avoid including FOUO information?				AR 25-1, Paragraph C-4e, question (26). Each Website must have a clearly defined purpose statement and Website plan that supports the organization's mission. (See Paragraph 2.1, Part II, DoD Web policy, and Paragraph 8-1c, DA PAM 25-1-1.) The Website plan is to be documented (see Paragraph 8-1c(4), DA PAM 25-1-1) along with the organization's continuity-of-operations plan (COOP), which must comply with Paragraph 6-1b, AR 25-1. Organizations must consult SMEs as to the markings on their Website purpose statements and plans, as they may require FOUO marking; if so, revisions will be needed for a version to be posted in the public domain.
1i. Does the publicly available Website plan address Webmaster / portal administrator contact information? 1j. Is the contact information generic rather than by-name (revealing PII)?				At minimum, this must include the Webmaster's / portal administrator's generic email address for users to request information or to direct questions, comments or suggestions for that organization, IAW Paragraph 5-5b(3), TR 25-1. Organizations will use organizational designation / title and generic position email addresses, such as office@organization.mil , IAW ASD-C3I memorandum, "Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites," Dec. 28, 2001, and TRADOC Command Guidance: Noble Eagle #02-019, "Personal Data on Unclassified Websites," March 13, 2002.

1k. Does the publicly available Website plan address procedures that explain posting of information and review of the site for content and format?				See Paragraph 8-1c(3), DA PAM 25-1-1.
1l. Has this explanation been reviewed for OPSEC indicators and sensitive information?				
1m. Does the publicly available Website plan address contingency and continuity of operations, describing what the organization will do with its Website during disasters or emergencies, and what important information and services will be provided to the public?				See Paragraph 5-5b(3), TR 25-1; Paragraph 8-1c(4), DA PAM 25-1-1; and Paragraph 6-1b, AR 25-1.
1n. Has the Website COOP on the Web been reviewed for OPSEC indicators and sensitive information?				
2a. Does the Website include from its homepage a description (or a link to the description from the homepage) of the organization's mission and the organization's structure?				See Paragraph 5-5b(2), TR 25-1, and Paragraph 8-2f(2), DA PAM 25-1-1. Names of personnel in an organization chart or section chart becomes a list of personnel names, which is prohibited.
2b. Does this description exclude names of personnel?				
Required notices: 3a. Are users of each publicly accessible Website provided with a privacy and security notice prominently displayed or announced on at least the first page of all major sections of each Web information service (WIS)?				AR 25-1, Paragraph C-4e, question (27). A WIS is a major division of content on a domain. Each WIS must contain on its first page / homepage the text, or a link to the text, of an approved privacy policy.
3b. Has the privacy/security notice been reviewed for OPSEC indicators and sensitive information?				
4a. Has the organization Website included a hyperlinks policy / notice?				If organizations use external links, they must 1) establish objective and supportable criteria or guidelines for how they select and maintain their links to non-Army Websites, and they must 2) post these criteria, along with an explanation of their process for linking to these sites, on their publicly accessible Website.
4b. Has this notice been reviewed for OPSEC indicators and sensitive information?				
Required Webpages: 5a. Does the Website include an "Important Notices" page?				The "Important Notices" page describes principle policies and other important notices that govern the Website, especially those mandated by law. (See Paragraph 8-2f(2)(k), DA PAM 25-1-1.)
5b. Has the "Important Notices" page been reviewed for OPSEC indicators and sensitive information?				
6a. Does the Website contain a Webpage, or link to a Webpage, labeled "Contact Us" or "Contact [organization name]"?				Each Website must post a "Contact Us" page and provide links to it from the homepage and every major point of entry on the Website, IAW Paragraph 8-2f, DA PAM 25-1-1. Contact information will be generic. The means to communicate via email will not be a by-name email address. If a Web-based contact form is employed, if PII is gathered, either a PAS or PA is required. See Paragraph 11.2, Part II, DoD Web policy.
6b. Has the "Contact Us" page been reviewed for OPSEC indicators and sensitive information?				
6c. Is the contact information provided generic in nature, rather than providing PII?				
6d. Does the contact Webpage include a means to communicate via email (organizational email address or Web-based contact form)?				
7a. Does the Website contain a Webpage labeled "About Us" or "About [organization name]"?				If the site is a main-entry-point Website, such as an organizational homepage, it must contain a Webpage labeled "About Us" or "About [organization name]." Paragraph 8-2f(2), DA PAM 25-1-1.
7b. Has the "About Us" page been reviewed for OPSEC indicators and sensitive information?				

7c. Does the "About Us" page include contact information, which may include generic email addresses, office phone number, office name, or an individual's title (no by-name email addresses or personal names)?				
8a. Does the Website contain a sitemap or subject index that gives an overview of the site's major content categories?				IAW Paragraph 8-2f(2), DA PAM 25-1-1.
8b. Has the sitemap or subject index been reviewed for OPSEC indicators and sensitive information?				
9a. Does the Website contain a "common questions" / FAQ page that provides basic answers to questions the organization receives most often?				IAW Paragraph 8-2f(2)(g), DA PAM 25-1-1.
9b. Has the "common questions"/FAQ page been reviewed for OPSEC indicators and sensitive information?				
10a. Does the Website include a "Help" page that outlines major proposed and implemented changes to the Website?				IAW Paragraph 8-3b(10), DA PAM 25-1-1.
10b. Has the "Help" page been reviewed for OPSEC indicators and sensitive information?				
Aggregation – pre-dissemination 11a. Has the OPSEC reviewer discussed with the content provider the form in which the proposed Web content will be distributed, the susceptibility of the information to data-mining, and the likelihood that the information could directly lead to the discovery and dissemination of knowledge that is otherwise controlled (e.g., classified information or FOUO information)? 11b. Does the reviewer's risk assessment consider the increased sensitivity of the organization's proposed information added to its already posted information, as well as to related information (even if not FOUO), if electronically aggregated in significant volume?				
Operational information: 12a. Is operational information purged from publicly accessible Websites? I.e.: 12b. Have analysis, plans, or recommendations concerning lessons-learned which would reveal sensitive military operations, exercises, vulnerabilities, or state of unit readiness been identified and prohibited / removed from being posted? <i>Includes OPORDs, OPLANs, CONOPs, SOPs, TTP, Army lessons-learned, AARs, planning guidance, detailed budget reports, inventory reports, detailed unit organization, detailed mission statement, specific unit phone/fax numbers (secure and unsecured), Time-Phase Force Deployment Data (TPFDD), operations schedules, logistics-support requirements, logistical posture, force apportionment, force allocation, unit bed-down information, unit augmentation, force synchronization, counter-terrorism measures, ISR capabilities and resources available to support the commander, vulnerabilities to exploitation or destruction of friendly ISR capabilities, C4I architecture and capabilities, weapons movements, mobilization information, communications methods, specific courses of action (CoAs) that forces are planning or cannot undertake/execute, command arrangements for executing CoAs, command-post locations and vulnerabilities, communications limitations, speed of deployment / redeployment of ground and air forces, ground/air/sea lines of communication (LOCs), locations of storage depots/ports/airfields, vulnerabilities to interdiction of the LOCs, critical item shortages (in all supply classes), limitations to resupply capability, vulnerabilities of defensive dispositions, vulnerabilities of sensors and other capabilities to detect attack, vulnerabilities to attack, vulnerabilities in protection or security forces or security plans.</i>				AR 25-1, Paragraph C-4e, question (32). IAW Paragraphs 3.5.3.1, Part II, 3.5.3.2, Part II, and 2.1, Part V, in the DoD Web policy, military plans, operations and exercises may be FOUO, and can also be categorized as "sensitive" (AR 530-1) or "critical" (AR 380-5) information. See AR 530-1, Chapter 5 of AR 380-5, Paragraph 2, Part V, in the DoD Web policy, and memorandum from the Deputy Secretary of Defense, "Information Vulnerability and the Worldwide Web," Sept. 24, 1998. See annexes for more examples of critical, sensitive, CUI, and FOUO information.

<p>12c. Has unclassified information that would reveal "sensitive movements of military assets or the location of units, installations or personnel where uncertainty regarding location is an element of the security of a military plan or program" been identified and prohibited / removed from being posted?</p> <p><i>Includes forces earmarked for possible CoAs, specific current force/unit locations, specific projected force/unit locations and alternate force/unit locations, current or future locations of unit commanders, current or future command-post locations, communications site locations, specific locations of exercises and operations and specific locations of forces participating in those exercises/operations, contents of Army Prepositioned Stocks (APS) and significant restructuring of APS, levels of supplies available for immediate support, pre-positioned supply sites, period of combat sustainment with those supplies, demand level for Class IX items, locations of ISR capabilities, ongoing ISR operations and their goals.</i></p>			<p>AR 25-1, Paragraph C-4e, question (32).</p> <p>IAW Paragraphs 3.5.3.1, Part II, 3.5.3.2, Part II, and 2.1, Part V, in the DoD Web policy, military plans, operations and exercises may be FOUO, and can also be categorized as "sensitive" (AR 530-1) or "critical" (AR 380-5) information. See AR 530-1, Chapter 5 of AR 380-5, Paragraph 2, Part V, in the DoD Web policy, and memorandum from the Deputy Secretary of Defense, "Information Vulnerability and the Worldwide Web," Sept. 24, 1998. The examples listed here are all "critical" information. See appendices for more examples of critical, sensitive, CUI, and FOUO information.</p>
<p>12d. Has personal information about U.S. citizens, DoD employees, and military personnel been identified and prohibited / removed from being posted?</p> <p><i>PII includes, but is not limited to: name, date of birth, place of birth, age, home address, race, email address containing personal name, Social security number, marital status, names/locations/any other identifying information about family members of DoD employees or military personnel (including family-member information within permitted biographies), biographies of people who are not official/designated command spokespersons, photographs of personnel, description of personnel, personal daily or travel schedules, military rank, civilian grade, official title, salary/pay information, telephone numbers other than numbers of duty offices, medical information, mother's maiden name, biometric records, rosters/lists of names, directories (including telephone directories) with names, charts with names, unit recall rosters, detailed duty rosters with names.</i></p>			<p>AR 25-1, Paragraph C-4e, question (32).</p> <p>A number of documents identify PII, which has been called both FOUO and "sensitive," and is prohibited on the publicly accessible Web unless for an official, designated command spokesperson and/or a GO or SES. (And in those cases, their marital status and family-member information is prohibited.) References are: Enclosure 2, DoDD 5400.11; OMB M-07-16; OSD memorandum, "Withholding of Personally Identifying Information Under the Freedom of Information Act (FOIA)," Nov. 9, 2001; memorandum from the ASD-C3I, "Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites," Dec. 28, 2001; Part III and Paragraph 2.2, Part V, DoD Web policy; memorandum from the DEPSECDEF, "Information Vulnerability and the Worldwide Web," Sept. 24, 1998; key management control list, Appendix C, AR 25-1; TRADOC Command Guidance: Noble Eagle #02-019, "Personal Data on Unclassified Websites," March 13, 2002; Army Web content and OPSEC training module, https://iatraining.us.army.mil. See Appendix G listing examples of FOUO information for more details.</p>
<p>12e. Has technological data been identified and prohibited / removed from being posted?</p> <p><i>Includes weapon schematics, electronic wire diagrams, frequency-spectrum data, weapons-systems development schedules (dates, times, locations), emerging technologies applicable to new weapons systems, computer software used in weapons-systems development / testing / evaluation, specific characteristics and capabilities of weapons and electronic systems available to coalition forces (and doctrine for using various weapons), new weapons that are available or are being employed, vulnerabilities and limitations in friendly weapons and weapons systems, location of unclassified computer databases used by the RDT&E community, specific contract criteria stated in a classified contract, identification of special-access elements within a contract or program, specific program protection plan (PPP) implementation methods.</i></p>			<p>AR 25-1, Paragraph C-4e, question (32).</p> <p>These categories are, at minimum, FOUO or sensitive information, or may refer to classified information, become classified by compilation, or be national-security information. OPSEC and security reviewers must review official information intended for public release pertaining to military matters, national-security issues, or subjects of significant concern to DoD, IAW DoDD 5230.9 and DoDI 5230.29. This includes information regarding military operational plans. Special attention must be given to unclassified information pertaining to classified programs. Reviewers must consider if there is a likelihood of</p>

				classification by compilation. Most categories in DoDI 5230.29 are releasable only by the Office of the Secretary of Defense; see Chapter 5, AR 360-1.
13a. Are OPSEC tip-off indicators purged from the organization's publicly accessible Website? I.e.:				AR 25-1, Paragraph C-4e, question (33). See Appendix H for more examples of OPSEC indicators.
13b. Are administrative tip-off indicators purged from the Website, such as personnel travel (personal and official business); attendance at planning conferences; commercial-support contracts; and FOUO?				
13c. Have operations, plans and training tip-off indicators been purged from the Website, such as (may overlap with categories in Q12) operational orders and plans; mission-specific training; critical maintenance, exercise and simulations activity; exercise, deployment or training schedules; unit relocation/deployment; inspection results, findings and deficiencies; and unit vulnerabilities or weaknesses?				AR 25-1, Paragraph C-4e, question (33). See appendices for more examples of OPSEC indicators, as well as more examples of critical, sensitive, CUI, and FOUO information.
13d. Have communication tip-off indicators been purged from the Website, such as spectrum emissions and associated documentation; changes in activity or communications patterns; increased use of Internet and/or e-mail by unit personnel, such as special Webpages posted by unit personnel and/or more email traffic for personal or official business; availability of secure communications; hypertext links with other agencies or units; family-support plans; and unofficial use of Instant Messenger, chat forums or bulletin board postings/messages between Soldiers and family members?				AR 25-1, Paragraph C-4e, question (33). See appendices for more examples of OPSEC indicators, as well as more examples of critical, sensitive, CUI, and FOUO information.
13e. Have logistics/maintenance tip-off indicators been purged from the Website, such as supply and equipment orders/deliveries; transportation plans; mapping, imagery and special documentation support; maintenance and logistics requirements; and receipt or installation of special equipment?				AR 25-1, Paragraph C-4e, question (33). See appendices for more examples of OPSEC indicators, as well as more examples of critical, sensitive, CUI and FOUO information.
Keyword search: 14. Has the Website reviewer performed a keyword search for any of the following documents and subsequently removed sensitive personal or unit information from publicly accessible Websites? Deployment schedules Duty rosters Exercise plans Contingency plans Training schedules Inspection results, findings and deficiencies Biographies Family support activities Phone directories Lists of personnel				AR 25-1, Paragraph C-4e, question (34).
OPSEC assessment IAW OPSEC methodology: 15a. Has the OPSEC reviewer performed the five-step OPSEC assessment in identifying, analyzing and protecting critical information? (Critical information is information about friendly activities, intentions, capabilities or limitations that an adversary needs to gain a military, political, diplomatic or technological advantage.) 15b. Has the OPSEC reviewer examined the information for the presence of any information requiring protection or other				Per DA policy, OPSEC/security reviewers are to conduct quarterly reviews of their organization's Website for possible critical or sensitive information already posted. The minimum review will include Website management control checklist items in AR 25-1, Appendix C. However, AR 25-2, Paragraph 4-20g(11), requires OPSEC and PAO review before

<p>information qualifying as exempt from public release?</p> <p>15c. Has the OPSEC reviewer screened proposed content for PII? Aggregation of names across pages must specifically be considered; name data can be compiled easily using simple Web searches.</p> <p>15d. Has the OPSEC reviewer screened proposed content for critical or sensitive information that has already been compromised (as this provides further unnecessary exposure of the compromised information and may serve to validate it)?</p>				<p>information is disseminated. IAW AR 530-1, this assessment is to be accomplished IAW OPSEC methodology. This part of the checklist is to aid OPSEC reviewers in their assessments IAW AR 530-1.</p>
<p>15e. Has the OPSEC reviewer assessed the risk on any FOUO information proposed for release?</p> <p><i>Includes proprietary information; test and evaluation information; technical information; information that would facilitate circumvention of DoD, component, or command policies, rules, regulations, or other significant guidance (for example, orders, manuals, instructions, or security classification guides); unclassified information that requires special handling; documents or information protected by a copyright; draft publications such as policies and regulations; and movement and readiness data.</i></p>				<p>Normally, posting FOUO information on the publicly accessible Web is prohibited. (See DoD Web policy.) FOUO may not be released to the public without undergoing a FOIA and SJA review, as well as OPSEC and PAO review. The OPSEC reviewer will not assume that records without FOUO markings do not contain FOUO information. Special attention must also be given to the increased sensitivity of information, even if not FOUO, if it can be electronically aggregated in significant volume. See Appendix G for more examples of FOUO information.</p>
<p>15f. Are requested exceptions to policy accompanied by a formal risk assessment required to assess the value of the information, the threat to the DoD Webserver environment and the information contained thereon, and the countermeasures employed by the DoD Webserver environment?</p>				<p>Exceptions to policy can be submitted to PAO for approval to publicly release, but the request for exception must be accompanied by a strong justification and a formal risk assessment from the OPSEC reviewer. In cases where the content is a risk to persons and not to a DoD Webserver, the risk assessment will focus on the value of the information.</p>
<p>15g. Has the OPSEC reviewer reviewed both single photographs and collections of images to screen photographs displaying critical or sensitive information?</p> <p>--Review single photographs, especially photos depicting the subjects including, but not limited to, the sensitive-photo listing in Appendix I.</p> <p>--Review other images such as detailed maps and detailed organizational charts.</p> <p>--Review directories or collections of photographs for risk in the aggregate.</p> <p>--Review the organization's multimedia / VI products for any still photography of prohibited subjects.</p>				<p>Beware of backgrounds, which may seem innocuous, on photos; good photo-editing software can magnify the background information enough to where an adversary can learn information from background walls, easels, computer screens, etc. See Appendix I listing examples of sensitive information for photo subjects that DoD and Army leaders have deemed sensitive.</p> <p>Collections / directories of photographs that could display critical or sensitive information upon aggregation should be secured in a private Website.</p>
<p>Management</p> <p>16. Has the organization supplemented DoDD 5205.02 (Paragraph 5.3.3) and DoD 5205.02-M (Enclosure 5), and issued procedures for a formal review of content for critical information, sensitivity, sensitivity in the aggregate, determination of appropriate audience, and distribution and release controls when releasing information?</p>				<p>Appendix 1 to Enclosure 3, DoD-M 5205.02-M, DoD Operations Security (OPSEC) Program Manual.</p>
Security reviewer				
<p>17. Has the security reviewer reviewed specifically for classified information?</p>				<p>Classified information includes official information regarding the national security that has been designated top secret, secret, or confidential IAW EO 12356. Classifications are: confidential, if the information could reasonably be</p>

				expected to cause damage to the national security if unauthorized disclosure occurs; secret, if the information would cause serious damage to the national security, and top secret, if the information would cause exceptionally grave damage.
18. Has the security reviewer assessed whether unclassified information pertaining to classified programs may become classified by compilation?				The security review should consider the likelihood of the information, if compiled or aggregated with other information likely to be posted on publicly accessible Websites, revealing an additional association or relationship that meets the standards for classification under DoD 5200.1-R.
19. Has the security reviewer used advanced search engines (e.g., high-end natural-language-based systems optimized for English syntax analysis) and other automated means to help assess whether the likelihood of information already on the public Web will cause the proposed information to become classified by compilation?				
20. Has the security reviewer provided an assessment or a statement that none of the content is classified or classified by compilation?				
21. Has the security reviewer reviewed proposed content for national-security information IAW AR 380-5 and as listed in DoDI 5230.29?				National-security information pertains to military matters, national-security issues, or subjects of significant concern to DoD. The term "national security information" encompasses classified information but also includes CUI, which includes FOUO and "sensitive but unclassified" information, IAW 380-5. National-security information includes military plans, weapons systems or operations; foreign-government information; intelligence activities (including special activities), intelligence sources or methods, or cryptology; foreign relations or foreign activities of the United States, including confidential sources; scientific, technological, or economic matters relating to the national security; U.S. government programs for safeguarding nuclear materials or facilities; or vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security. See appendices for more examples of critical, sensitive, CUI, and FOUO information.
22. If national-security information is present, has the security reviewer advised the content provider that this information must be cleared by HQ DA and OSD, and thus forwarded to Army OCPA through TRADOC PAO?				

Legal Counsel's Review Checklist				
Use this checklist to check compliance with federal, DoD, Army, and TRADOC publicly accessible Web policies.				
Name of Reviewer		Date of Review		
URL of Webpage Reviewed		Organization Webmaster Name / Email Address / Phone Number		
Department / Organization Name		Content Provider Name / Email Address / Phone Number OR Organization Website Coordinator Name / Email Address / Phone Number		
Issue / Concern	Yes	No	N/A	Notes / Comments
Pre-dissemination issues: 1a. Has content been reviewed by legal counsel if there appear to be copyright, trademark, conflict-of-interest, or other ethical issues in the proposed content? 1b. If so, does the submission request to PAO include a summary of the legal counsel's opinion or a statement from counsel that there are no legal issues in this content?				PAO, in determining whether to release information to the public, needs legal counsel's review if the content proposed for posting may have copyrighted or trademarked material, may present conflict-of-interest issues, or may have other ethical issues.
2a. Has legal counsel advised the organization on use of copyrighted material? 2b. Has legal counsel ensured that the organization has obtained the copyright owner's written permission if the organization proposes to use copyrighted information? 2c. Has legal counsel ensured that the organization has established a procedure with the original content owner for updating any information and for periodically verifying its releasability, currency, and accuracy?				See Paragraphs 2.3 and 3.5.5, Part II, DoD Web policy.
3a. Has content been reviewed by legal counsel if an organization is requesting to post FOUO information as an exception to policy? 3b. If so, does the submission request for content review include the legal counsel's opinion?				IAW Paragraph 1-5c(3)(e), AR 530-1.
4. If the organization plans to use frames to link to external sites, has the organization consulted legal counsel concerning trademark and copyright issues before establishing such links?				IAW Paragraph 7.1.5, Part II, DoD Web policy.
Post-dissemination issues: 5. If a copyright notice is present on an organization's Webpages, has legal counsel advised organizations remove it?				U.S. government works are not eligible for copyright protection.
6a. If an organization has republished a copyrighted news story, has legal counsel queried whether the organization has written approval from the news source? 6b. If the organization has not obtained written approval, has legal counsel advised the organization to remove the story from its Website? 6c. Has legal counsel advised the organization about "fair use"? 6d. Has legal counsel advised the organization that it may link to the original news source if it includes the prescribed DoD external-links disclaimer?				There are several strictures on copyrighted material: organizations must obtain written approval before using copyrighted material; the materials must relate to the organization's mission; and there must be an established procedure for updating and verifying the copyrighted information. See Paragraphs 2.3 and 3.5.5, Part II, DoD Web policy.

7. Has content been reviewed by legal counsel if the organization plans to post the content in an AKO unrestricted-content area?				IAW Paragraph 2-3a(15), AR 530-1, and Paragraph 6-7c(3), AR 25-1.
Multimedia / VI-specific issues: 8a. Has legal counsel reviewed multimedia / VI productions and ensured that there are no legal encumbrances? 8b. Has legal counsel ensured that the organization has obtained all required releases for the production? 8c. Has legal counsel ensured that the contractor has assigned all interest in the work to the government?				IAW Paragraphs 7-10b(4)i, 7-10b(4)k, 7-10b(4)l, AR 25-1.
9. Does the Website use only text or hyperlinked text (no graphics / logos) to direct users to non-Army software download sites?				IAW Paragraph 8-1k, DA PAM 25-1-1. This is an endorsement / conflict-of-interest issue; IAW the JER, conflicts of interest include product endorsements or preferential treatment of any private organization or individual – these are prohibited on a DoD Website.
Political issues: 10a. Does the Website avoid making links to a political campaign, committee, or lobby? 10b. Does the Website avoid linking to the post's civilian-enterprise (CE) on-line newspaper if the newspaper includes paid political advertisements or advertisements that advocate a particular position on a political issue?				IAW Paragraph 8-2b(2), DA PAM 25-1-1. IAW Paragraph 3-4e(1), AR 360-1, personnel acting in their official capacity may not engage in activities that associate DoD with any partisan political campaign or election, candidate, cause or issue. See Paragraph 3-4e(5), AR 360-1.
10c. Does the post's on-line CE newspaper avoid carrying paid political advertisements or advertisements that advocate a particular position on a political issue? 10d. Does the on-line CE newspaper avoid conducting or publishing any polls, surveys, or straw votes relating to political campaigns, elections, candidates, causes or issues?				IAW Paragraphs 3-4e(5) and 3-4e(6), AR 360-1.

Quality of Information (QI) Review Checklist Use this checklist to prompt reviewers to check content for compliance to QI standards established by law or best practice. Checklist can be used in either pre-dissemination or post-dissemination reviews.				
Name of Reviewer		Date of Review		
URL of Webpage Reviewed		Organization Webmaster Name / Email Address / Phone Number		
Department / Organization Name		Content Provider Name / Email Address / Phone Number <u>OR</u> Organization Website Coordinator Name / Email Address / Phone Number		
Issue / Concern	Yes	No	N/A	Notes / Comments
1a. Has content been reviewed for objectivity (neutrality, accuracy, reliability) IAW QI standards?				"Objectivity" is in two parts: 1) whether the information itself, as a matter of substance, is accurate, reliable, and unbiased, and 2) on if its presentation is accurate, clear, complete, and unbiased. "Utility" refers to the usefulness of the information to intended users, including the general public . "Integrity" concerns information assurance (IA), as the standard refers to the protection of information from unauthorized access or revision to ensure that the information is not compromised through corruption or falsification.
1b. Has content been reviewed for utility (timeliness, relevance, Section 508 compliance) IAW QI standards?				
1c. Has content been reviewed for integrity (secure, protected on server) IAW QI standards?				
2a. Has scientific, technical, or financial information undergone a security review?				
2b. Has scientific, technical, or financial information undergone a peer review?				
2c. If scientific, technical, or financial information is "influential," has it undergone an advanced-level review and able to meet the standard of "substantially reproducible"?				
3. Have images (e.g., photographs, graphic arts) been reviewed for journalistic quality?				
4. Has the content been reviewed for Section 508 compliance and other accessibility / usability concerns?				
5a. Does the content adhere to published DoD and Army policies?				
5b. Does the content avoid including anything of questionable value to the general public, such as facetious humor, which is subject to possible misunderstanding or misinterpretation?				
5c. Has the information been copy-edited and spell-checked?				
5d. Does the homepage content avoid including abbreviations? Abbreviations may be used on other pages if words are spelled out first.				
6. Does the submission to PAO requesting clearance to post include a summary of what QI review(s) have been performed?				

Checklist for Public Affairs Reviewers

See Paragraph C-4e, Appendix C, AR 25-1, for checklist of all key management controls as well as Paragraph 6-7, AR 25-1. This checklist covers required content on DoD / Army / TRADOC Websites, as well as content prohibited on DoD / Army / TRADOC Websites. PAO reviewers should review the other reviewers' checklists as well as use the following one tailored for PAOs. **(Note: The following checklist should be used in lieu of one prepared and disseminated by TRADOC PAO early in 2006.)**

This checklist is suggested for use by organization leaders, Webmasters, and Public Affairs officers to determine if Websites and Webpages meet DoD, Army, and TRADOC content policies, either pre- or post-dissemination of information; the completed checklist can also be sent to TRADOC PAO as a pre-dissemination approval / clearance tool when an organization is establishing a new Website or making major changes to an existing one.

If the latter, send to TRADOC PAO's content-review email address, monr.contentreview@monroe.army.mil, or to TRADOC PAO's generic email address, tradocpao@monroe.army.mil. PAO reviewers review and approve for release any new content to be posted on an organization's corporate Website and to AKO areas accessible to all account types. PAO new-content review will be conducted for 1) establishments of new Websites, 2) new Webpages or documents, and for 3) major updates of Websites. PAO reviewers will also conduct quarterly reviews of updated content after the content has been posted.

Name of Reviewer		Date of Review		
URL / Proposed URL		Organization Webmaster Name / Email Address / Phone Number		
Department / Organization Name		Content Provider Name / Email Address / Phone Number OR Organization Website Coordinator Name / Email Address / Phone Number		
Check One: New Website [] Site Major Change [] New page [] Page Revision [] Summarize New Content or Changes Here:		Target Date for Information to be Posted		
Issue / Concern (reviewer may wish to add comments in the blocks along with the issue / concern)	Yes	No	N/A	Notes / Comments
Pre-dissemination review checks and procedures				
1a. Has the content provider / Website coordinator been advised at what level that review and clearance of content can be made?				Paragraphs 5-3c(1), 5-3c(2), 6-6b, 6-7b, and 6-9a, AR 360-1.
1b. Has any information that must be cleared by HQ DA, OSD, or OSR been submitted to the proper clearance authority?				Paragraphs 2-2c(2) and 2-2c(3), AR 360-1.
1c. Has the organization included a recommendation on the releasability of any information submitted to OSR?				DoDI 5230.29. See Paragraphs 6-1c and 6-7b, AR 360-1.
1d. Has any military-intelligence and security-related information, photographs, video, and audiotapes been reviewed and authorized for release by INSCOM?				Paragraph 5-3c(5), AR 360-1.

1e. Has any operational information pertaining to Special Operations Forces (SOFs) been reviewed and authorized for release by USASOC?				Paragraph 5-3c(6), AR 360-1.
1f. Have reviews by all appropriate command / CoE experts been performed (e.g., OPSEC, legal, QI)?				Paragraph 5-4a, AR 360-1.
1g. Is the content of value to the general public?				Refer any information not designed for reaching the public at large (i.e., is of value to Army personnel only) for placement in the organization's portal, on restricted areas within the portal, or on AKO knowledge centers / communities of practice, AKO team sites, TKE, or BCKS, as appropriate.
1h. Is there a valid mission need to disseminate it?				
1i. Has the head of the organization, or his / her authorized representative, approved the defined purpose and general content of his / her organizational Website?				Paragraph 8-2g, DA PAM 25-1-1.
Personally identifiable information (PII)				
2a. Does any of the proposed content contain PII?				
2b. Do organizational directories list organizational titles and generic email addresses rather than names of individuals and by-name email addresses?				See Paragraph 6-7c(4)(i), AR 25-1; "Memorandum from ASD-C3I, "Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites," Dec. 28, 2001; and TRADOC Command Guidance: Noble Eagle #02-019, "Personal Data on Unclassified Websites," March 13, 2002.
2c. Has a biography been submitted for posting?				IAW AR 25-55, Paragraph 3-200, under exemption No. 6, "By DoD policy, the names of general officers (or civilian equivalent) or [PAOs] may be released at any time." Family-member information is prohibited PII.
2d. If so, is it that of an official, designated command spokesperson and / or any GO or SES?				
2e. Do permitted biographies exclude personal email address, home address, home telephone number, Social Security number, date of birth, or reference to family members?				
2f. Do all documents containing individual names (excepting official command spokespersons) include an application for exception to policy (with strong justification)?				
2g. Do requests for persons to be designated as official command spokespersons (thereby permitting their biographies) include strong justification?				
2h. If session cookies are used on this Website to collect PII about Web visitors, is there a Privacy Advisory (PA) or Privacy Act Statement (PAS)?				See Paragraph 11.2, Part II, DoD Web policy.
Duplication of information				
3a. Does the organization wish to re-post / duplicate information found on another federal site?				IAW DoD Web policy, the organization's Web content should be limited to only information for which it is responsible. The organization should provide links to documents that other organizations originate, rather than re-post / duplicate documents on the local Webserver.
3b. If so, has the organization compellingly justified its reasons in writing as part of the pre-dissemination content-review process?				
3c. Are the organization's reasons for performance, security, or other mission-related reasons?				
3d. Will Army regulations, publications, forms, or other Army-wide publications be linked to on the Army Publishing Directorate site				

rather than duplicated locally?				
3e. Has the owner of the original content given written permission to replicate the information?				
3f. Is a copy of this written permission included in the request for content review?				
Copyrighted material				
4a. Has express written permission from the copyright owner been obtained for proposed content that is copyrighted?				IAW DoD Web policy.
4b. Has the organization established a procedure with the copyright owner for updating / periodically verifying the information?				
4c. Has the organization wishing to post copyrighted information consulted legal counsel?				
4d. Has a copy of legal counsel's opinion been included as part of the content-review submission request?				
Official imagery				
5. Does official DoD imagery conform to DoDD 5040.5?				
On-line civilian-enterprise (CE) post newspapers				
6a. Has the content of on-line CE newspapers been specifically reviewed for endorsement issues, including Soldiers appearing in uniform in commercial advertising or actors / models posing as Soldiers in uniform?				Models cannot wear "distinctive" parts of uniform while portraying Soldiers. See Paragraph 3-2, AR 360-1; Paragraph 3-209, JER; Paragraph 1-4d and Paragraph 1-12, AR 670-1; Paragraph (f), 10 USC 772.
6b. Do Army-funded newspapers and editorial content of CE publications comply with DA PAM 25-1-1, 8-2h?				
FOUO				
7. If the organization proposes to post FOUO as an exception to policy, has the organization consulted legal counsel as well as a certified OPSEC officer IAW AR 530-1?				The organization should submit strong justification and the organizational OPSEC officer's risk assessment to legal counsel as well as to PAO.
Forms and publications				
8a. Does the Website provide easy access to on-line customer services and forms?				IAW AR 25-1 and DA PAM 25-1-1.
8b. Are the services and forms applicable to the general public?				
8c. Is access to the services and forms displayed as prominently as possible?				
8d. Are the services and forms based on an analysis of customer needs?				
8e. Have the most frequently requested publications been placed in a portal?				
Website purpose, Website plan, organization mission, organization structure				
9a. Does the Website contain a clearly defined purpose statement that supports the organization's mission?				Each Website must have a clearly defined purpose statement and Website plan that supports the organization's mission. (See Paragraph 2.1, Part II, DoD Web policy, and Paragraph 8-1c, DA PAM 25-1-1.)
9b. Is the purpose statement backed by a Website plan that is approved by the organization's parent command or organization?				The Website plan is to be documented (see Paragraph 8-1c(4), DA PAM 25-1-1) along with the organization's continuity-of-operations plan (COOP), which must comply with Paragraph 6-1b,

9c. Is the Website plan publicly available on the organization's Website?				AR 25-1. Organizations must consult SMEs as to the markings on their Website purpose statements and plans, as they may require FOUO marking; if so, revisions will be needed for a version to be posted in the public domain.
9d. Does the publicly available Website plan address the Website's registration?				See Paragraphs 8-1c(1) and 8-1e, DA PAM 25-1-1; and Paragraph 6-7c(2), AR 25-1.
9e. Does the publicly available Website plan address Webmaster / portal administrator contact information?				At minimum, this must include the Webmaster's / portal administrator's generic email address for users to request information or to direct questions, comments or suggestions for that organization, IAW Paragraph 5-5b(3), TR 25-1. Organizations will use organizational designation / title and generic position email addresses, such as office@organization.mil , IAW ASD-C3I memorandum, "Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites," Dec. 28, 2001, and TRADOC Command Guidance: Noble Eagle #02-019, "Personal Data on Unclassified Websites," March 13, 2002.
9f. Does the publicly available Website plan address procedures that explain posting of information and review of the site for content and format?				See Paragraph 8-1c(3), DA PAM 25-1-1.
9g. Does the publicly available Website plan address contingency and continuity of operations, describing what the organization will do with its Website during disasters or emergencies, and what important information and services will be provided to the public?				See Paragraph 5-5b(3), TR 25-1; Paragraph 8-1c(4), DA PAM 25-1-1; and Paragraph 6-1b, AR 25-1.
9h. Does the Website include from its homepage a description (or a link to the description from the homepage) of the organization's mission and the organization's structure (excluding names of personnel)?				See Paragraph 5-5b(2), TR 25-1, and Paragraph 8-2f(2), DA PAM 25-1-1. Recommendation: Include purpose, mission, and vision on the "About Us" page (see "required pages" section below), but address all requirements in 7a through 7h via content on or links from the homepage.
Required notices: privacy notice				
10a. Are users of each publicly accessible Website provided with a privacy notice prominently displayed on at least the homepage and first page of all major sections of each Web information service?				IAW Paragraph 6, Part II, DoD Web policy, all publicly accessible Websites must have both a "human readable" privacy policy and machine-readable technology that automatically alerts users about whether site privacy practices match their personal privacy preferences. The privacy notice must be contained within the content of the "Important Notices" page; linking to the "Important Notices" page from the homepage and first page of all major sections of a Website helps ensure compliance with the privacy-notice requirement. A Web information service (WIS) is a major division of content on a domain

				such as www.tradoc.army.mil – each major division, for instance, would be represented by organizational Websites such as PAO, G-6, Chaplains, G-1/4, G-3/5/7, etc. Each WIS must contain on its first page / homepage the text, or a link to the text, of an approved privacy policy.
10b. Does the privacy policy describe how, in general, security is maintained on the site, what specific information is collected, why it is collected, and how it is used? (All information collected must be described in this policy.)				Paragraph 6, Part II, DoD Web policy.
10c. Is the link to the “human readable” version of the privacy policy labeled “Privacy policy”?				Paragraph 6, Part II, DoD Web policy.
10d. Does the privacy notice or link to the privacy notice avoid the perception of danger (i.e., skull-and-crossbones logos or “warning” graphics)?				Paragraph 6, Part II, DoD Web policy.
Required notices: external-links disclaimer				
11a. If external links are present, does the Website contain a “disclaimer for external links” notice or intermediate “exit notice” page when a user clicks on a link to any unofficial Website?				An external link is a link to any site outside the official DoD WIS – usually, but not restricted to, the .mil domain. The external-links disclaimer must be displayed when an organization links to an unofficial, “external” Website. The disclaimer must appear on the page / pages listing external links or through an intermediate “exit notice” page generated by the server. This standard applies to links from an official DoD site to any site other than an official DoD Website, IAW Paragraphs 7.1.6, 7.1.7, and 7.2, Part II, DoD Web policy, and Paragraph 6-7c(7)(c), AR 25-1.
11b. Is the disclaimer IAW Paragraph 7.2, Part II, DoD Web policy, and Paragraph 6-7c(7)(c), AR 25-1?: “The appearance of external hyperlinks does not constitute endorsement by the U.S. Army of this Website or the information, products, or services contained therein. For other than authorized activities such as military exchanges and MWR sites, the U.S. Army does not exercise any editorial control over the information you may find at these locations. Such links are provided consistent with the stated purpose of this Website.”				
Required notices: hyperlinks policy / notice				
12. Has the organization included a hyperlinks policy / notice?				<p>If organizations use external links, they must 1) establish objective and supportable criteria or guidelines for how they select and maintain their links to non-Army Websites, and they must 2) post these criteria, along with an explanation of their process for linking to these sites, on their publicly accessible Website. Organizations' linking procedures must explain why some links are chosen and others are not. (See Paragraph 8-1k, DA PAM 25-1-1, and Paragraph 6-7c(7), AR 25-1.) USA.gov's linking policy (http://www.usa.gov/About/Linking_Policy.shtml) is recommended as an example for developing Army public Website linking policies.</p> <p>External-links guidelines must consider the information needs of mission-related requirements and public-communications and community-relations objectives.</p>
Section 508				

13. Do videos include transcripts or captioning for the hearing impaired?				<p>Army Websites must be accessible to handicapped users IAW Section 508 of the Rehabilitation Act. Transcripts for videos, or captioning for the hearing impaired, are required. Other Section 508 compliance requirements are listed in the "required pages" section below. Because all Army Websites must be in compliance with Section 508 and must provide a link to the organization's accessibility policy from the "Important Notices" page (see Paragraph 8-3b(2), DA PAM 25-1-1), all TRADOC organizational Websites, not just HQ TRADOC, should include an "Important Notices" page.</p>
Required Webpages: "Important Notices" page				
14a. Does the Website include an "Important Notices" page?				<p>A link to the "Important Notices" page must be placed at the footer of every Webpage as well as being clearly accessible from the homepage. The "Important Notices" page describes principle policies and other important notices that govern the Website, especially those mandated by law. At a minimum, this page includes the requirements in 14c through 14f. (See Paragraph 8-2f(2)(k), DA PAM 25-1-1.)</p>
14b. Is it linked from the footer of every Webpage in the site, as well as being accessible from the Website's homepage?				<p>Links to other Webpages containing this information are acceptable (and in several cases, are desirable to avoid repetition, such as the content required on the "Contact Us" page), as long as the "Important Notices" page consolidates the links for the content required in 14c through 14f.</p>
14c. Does the "Important Notices" page include the organization's privacy policy, including its cookie policy?				<p>The cookie policy must state that the Website does not use "persistent" cookies or any other automated means to track the activity of users over time and across Websites.</p> <p>The privacy policy must state how security is maintained on the site, what specific PII is collected, why it is collected, and how it is used. All information collected must be described in this notice. (See Paragraph 6, Part II, DoD Web policy.)</p> <p>See the DoD standard notice for the text.</p>
14d. Does the "Important Notices" page include information on how Website visitors may request information under the Freedom of Information Act (FOIA)?				<p>Website visitors must be advised how to make FOIA requests. FOIA requests are made to one central email: FOIA@rmda.belvoir.army.mil.</p>
14e. Does the "Important Notices" page include the organization's accessibility (Section 508) policy?				<p>The Section 508 policy must be posted on this page or be linked from it. Text will advise Website visitors that it is the Army's policy that its Websites are accessible to handicapped users IAW Section 508 of the Rehabilitation Act; describe the site's compliance with</p>

				<p>Section 508; and inform visitors whom to contact for a Section 508 complaint. (Also see Paragraph 8-3, DA PAM 25-1-1.)</p> <p>When the Website includes electronic forms meant to be completed on-line, a form must also be offered to allow people using assistive technology to access the information, field elements and functionality required for completion and submission of the form, including all directions and cues.</p>
14f. Does the "Important Notices" page include the organization's Quality of Information (QI) guidelines?				<p>The QI policy will advise Website visitors, at minimum, that the organization's goal for its on-line information is accuracy, objectivity, and integrity, and that it undergoes technical, supervisory, editorial, or legal review as appropriate, based on the information's nature. Website visitors will also be given the generic contact information for the organization's information-quality POC.</p>
Required Webpages: "Contact Us" page				
15a. Does the Website contain a Webpage, or link to a Webpage, labeled "Contact Us" or "Contact [organization name]"?				<p>Each Website must post a "Contact Us" page and provide links to it from the homepage and every major point of entry on the Website, IAW Paragraph 8-2f, DA PAM 25-1-1. The page must be labeled "Contact Us" or "Contact [organization name]" and contact information will be generic. Army policy (see Paragraph 8-2f, DA PAM 25-1-1) requires the specific items of content in 10c through 10j on the "Contact Us" page.</p>
15b. Is the "Contact Us" page linked from the organization's homepage and every major point of entry?				<p>See Paragraph 8-2f, DA PAM 25-1-1.</p>
15c. Is the contact information provided generic in nature, rather than providing PII?				
15d. Does the contact Webpage include the organization's street address, including addresses for any regional or local offices?				
15e. Does the contact Webpage include office phone number(s), including numbers for any regional or local offices?				
15f. Does the contact Webpage include a means to communicate via email (organizational email address or Web-based contact form)?				<p>The means to communicate via email will not be a by-name email address. If a Web-based contact form is employed, if PII is gathered, either a PAS or PA is required. See Paragraph 11.2, Part II, DoD Web policy.</p>
15g. Does the contact Webpage outline the organization's policy and procedures for responding to email inquiries, including whether the organization will answer inquiries and the expected response time?				
15h. Does the contact Webpage contain contact information for the				

organization's QI Program POC?				
15i. Does the contact Webpage contain contact information (office names / titles / phone numbers) for small business to direct queries to?				Contact information (title / phone number) for small businesses is required by the Paperwork Reduction Act.
15j. Does the contact Webpage contain contact information for FOIA requests?				The means to request information through FOIA is also included on the "Important Notices" page. Instruct Website visitors on this page, too, to make FOIA requests by emailing FOIA@rmda.belvoir.army.mil .
Required Webpages: "About Us" page				
16a. Does the Website contain a Webpage labeled "About Us" or "About [organization name]"?				If a main-entry-point Website, such as HQ TRADOC, the Website must contain a Webpage labeled "About Us" or "About [organization name]"? HQ TRADOC subordinate organizations' Websites must contain a link to TRADOC's "About Us" page. Paragraph 8-2f(2), DA PAM 25-1-1, requires the specific items of content in 16c through 16l on the "About Us" page.
16b. Or, does the Website contain a link to TRADOC's "About Us" page?				
16c. Does the "About Us" page include a description of the organization's mission, including its statutory authority?				
16d. Does the "About Us" page include the organization's strategic plan (unclassified, sanitized version), vision, or set of principles?				
16e. Does the "About Us" page include the organization's structure, including basic information about the organization's parent and / or subsidiary organizations and regional / field offices?				
16f. Does the "About Us" page include contact information, which may include generic email addresses, office phone number, office name, or an individual's title (no by-name email addresses or personal names)?				
16g. Does the "About Us" page include information about professional opportunities / jobs at the organization?				Preference is to link to CPO on-line at http://acpol.army.mil/employment/index.htm .
16h. Does the "About Us" page contain a link to a sitemap or subject index for the Website?				
16i. Does the "About Us" page contain a link to a "common questions" / FAQ page?				
16j. Does the "About Us" page contain easy access to existing on-line citizen services and forms?				The organization's Website must contain easy access to any on-line citizen services and forms it makes available to the general public, and this access (link) must be displayed as prominently as possible. Access to on-line services and forms must also be linked from the "About Us" page.
16k. Does the "About Us" page contain a link to a portal for the organization's most frequently requested publications?				Each Website must organize its most frequently requested publications into a portal. The "About Us" page must contain a link to the publications portal. (However, do not duplicate content on

				the HQ TRADOC homepage or Army Publishing Directorate Website.)
16l. Does the "About Us" page contain a link to the "Important Notices" page?				
Required Webpages: sitemap or subject-index page				
17a. Does the Website contain a sitemap or subject index that gives an overview of the site's major content categories?				Each Website must include a site map or subject index that gives an overview of the Website's major content categories. At minimum, the sitemap must be linked from the homepage, IAW Paragraph 8-2f(2)(f), DA PAM 25-1-1.
17b. Is the sitemap or subject index linked to from the Website's homepage and its "About Us" page?				
Required Webpages: common questions / FAQ page				
18a. Does the Website contain a "common questions" / FAQ page that provides basic answers to questions the organization receives most often?				IAW Paragraph 8-2f(2)(g), DA PAM 25-1-1.
18b. Is the "common questions" / FAQ page linked to from the Website's homepage and its "About Us" page?				
"Help" page 19. Does the Website include a "Help" page that outlines major proposed and implemented changes to the Website?				IAW Paragraph 8-3b(10), DA PAM 25-1-1.
Search box / page 20. Does each page of the Website include either a search box or a link to a search page entitled "Search"?				Organizations must include either a search box or a link to a search page from every page of the Website. The search box or link will be entitled "Search." Webmasters will place subject and keywords in source code to aid content searches. Focused searches may be given to search within sets of information, databases or applications. Websites that are narrow in scope or less than 200 pages may substitute a sitemap or A-to-Z index rather than implement a search engine. (See Paragraph 8-3b(8), DA PAM 25-1-1. The paragraph also outlines minimum service-level standards for the search function.)
Required statements or other text				
21a. Has a currency declaration on every Webpage (i.e., "Last updated on ____") or a date stamp been included on each page to indicate when last altered or reviewed?				A currency declaration is required on every Webpage: "Army public Websites will clearly state the date the content was posted or updated for every Webpage indicating to visitors that the content is current and reliable." Webmasters must include a statement such as "Last updated on ____" or a date stamp on each page to indicate when last altered

21b. When was the content last reviewed, including for accuracy and timeliness?				or reviewed, IAW Paragraph 8-11, DA PAM 25-1-1. The author of / POC for a publicly accessible Webpage should give generic email address contact information or a generic "mailto:" link (such as monr.webmaster@monroe.army.mil) for Website visitors to contact if they find content to be incorrect or outdated.
21c. Does each Webpage state the organization's official name and display the phrase "This is an official U.S. Army site"?				Each Webpage must state the organization's official name and display the phrase "This is an official U.S. Army site." Homepages and second-tier pages must also include the organization's name identified as the site sponsor as part of the page title, IAW Paragraph 8-11, DA PAM 25-1-1, and Paragraph 5-5b(5), TR 25-1.
21d. Do homepages and second-tier pages also include the organization's name identified as the site sponsor as part of the page title?				
21e. Has a redirect notice / page been provided when links have been changed?				When Webpages are deleted, the Webmaster must 1) delete links from pages containing links to the page being deleted; 2) delete any associated files such as Word documents or images from the Webserver; and 3) use a redirect notice / page to provide Website visitors with substitute links or content when page destinations are changed by deleted Webpages.
Required links (required by Army and TRADOC policy)				
22a. Does the HQ TRADOC homepage link to USA.gov ?				Major organizational pages like HQ TRADOC must link to USA.gov from their homepage. The entry for the link shall read "USA.gov: U.S. Government Web Portal," IAW Paragraph 8-5d, DA PAM 25-1-1. Unless the organization is Army, Army-command or HQDA-staff-element level, a link to USA.gov is not required.
22b. Does the entry for the link read "USA.gov: U.S. Government Web Portal"?				
22c. Is a link to the FAQ page provided from the "About Us" page?				IAW Paragraph 8-2f(2)(g), DA PAM 25-1-1.
22d. Is a link to the portal for most frequently requested publication(s) provided from the "About Us" page?				IAW Paragraph 8-2f(2)(j), DA PAM 25-1-1.
22e. Is there a link to the "Important Notices" page at the footer of every Webpage?				IAW Paragraph 8-2f(2)(k), DA PAM 25-1-1.
22f. Is a link from the homepage provided to the "Help" page?				IAW Paragraph 8-3b(10), DA PAM 25-1-1.
22g. Is there a link from the homepage to the sitemap or subject index page?				IAW Paragraph 8-2f(2)(f), DA PAM 25-1-1.
22h. Is there a link from the homepage (at minimum; can be elsewhere through the site) to the next senior Website in the hierarchy?				All TRADOC sites must link to: the next senior Website in the hierarchy IAW TR 10-5; the organizational homepage on AKO if one exists; the TRADOC logo and motto; the HQ TRADOC homepage; and the Army homepage, IAW Paragraph 5-5b(1), TR 25-1.

22i. Is there a link from the homepage (at minimum) to the organizational homepage on AKO if one exists?				If the organizational homepage is access-controlled beyond basic AKO authentication, there must be the appropriate disclaimer on the public site, near the link to AKO, per DoD Web policy.
22j. Is there a link from the homepage (at minimum) to the TRADOC logo and motto?				IAW Paragraph 5-5b(1), TR 25-1.
22k. Is there a link from the homepage (at minimum) to the HQ TRADOC homepage?				IAW Paragraph 5-5b(1), TR 25-1.
22l. Is there a link from the homepage (at minimum) to the Army homepage?				IAW Paragraph 5-5b(1), TR 25-1.
22m. Is there a link from the homepage to the organization's portal for its most frequently requested publications?				IAW Paragraph 8-2f(2)(j), DA PAM 25-1-1.
22n. Does each Webpage link back to the Website's homepage and to its parent organization's homepage?				To improve Website utility, each Webpage must link back to the Website's homepage and to its parent organization's homepage, IAW Paragraph 8-5c, DA PAM 25-1-1.
External-links policy (an external link is a link to any Website other than an official DoD Website)				
23a. Do links to documents requiring downloading provide enough contextual information that visitors have a reasonable understanding of what to expect when they view the material after downloading?				IAW Paragraph 8-3b(5), DA PAM 25-1-1.
Graphical links 23b. If an organization uses a graphical link, does that link also contain text indicating what it links to?				IAW Paragraph 8-5c, DA PAM 25-1-1.
23c. Do links use only text to direct visitors to non-Army software download sites, avoiding company graphics or logos as graphical links?				
Overall quality 23d. Are both internal and external links current and accurate?				Organizations must avoid linking to external sites unless they are related to the organization's mission or function, or might be seen as being related. See Paragraph 8-1k, DA PAM 25-1-1, and Paragraph 6-7c(7), AR 25-1.
23e. Are the external links present required by organization's mission?				
23f. Do the links have continued suitability?				
23g. Are external links chosen fairly and in the best interest of the public?				
23h. Do external links avoid requiring or encouraging users to choose any browser-specific software?				
23i. Do listings of Web links separate external Web links from government and military links?				Paragraph 6-7c(7)(b), AR 25-1.
23j. Do official Websites avoid linking to an unofficial Website not in compliance with Web policy?				
23k. Do the links avoid product endorsements or preferential treatment?				
23l. If the organization is using frames to link to external sites, has the organization consulted legal counsel concerning trademark and				

copyright issues?				
23m. Do Webpages link to a government-wide portal or site from their pages on a similar topic?				
23n. When a government-wide portal or specialized Website is available on a subject that the public would expect to find on an organization's site but the organization does not provide that information, is there a link to the government-wide portal or site in a logical and useful location?				
Standard navigation				
24. If the organization is exempt from using TRADOC G-6's Webpage template, has consistent navigation between and within pages been established?				<p>Standard navigation criteria, IAW Paragraph 8-3b(7), DA PAM 25-1-1:</p> <ul style="list-style-type: none"> Common items appearing on most Webpages will be in the same location on each page and have the same appearance and wording. A navigation item that is shared by a group of pages (such as a set of pages on a single topic, or for a division of the organization) will also have the same location, appearance, and wording on each page. Navigation items of the same type will look and behave like each other. For example, if a set of pages on one topic has subtopic links in the left navigation bar, pages on other topics will have subtopic links in the left navigation bar that are similar. If a set of Webpages requires specialized navigation, that navigation is applied to the largest possible local grouping (such as a topic, an audience or a complete organizational unit). The specialized navigation will be similar in appearance and behavior to the overall navigation scheme.
Corporate ethos				
25a. Do the TRADOC homepage and pages linked off the TRADOC homepage include the command's major communication themes?				<p>As tools of public and command information, Army Websites must display the concepts of "branding" and "speaking with one voice." Many of the required links and Webpages not only enhance visitor usability but also enhance the Army's corporate ethos. "Yes" answers in this section help ensure the organization's Website displays corporate ethos; for most questions, "no" answers indicate non-compliance to DoD / Army / TRADOC policy.</p>
25b. Do TRADOC subordinate command and Center of Excellence / school homepages incorporate TRADOC and local communication themes into Website displays?				IAW Paragraphs 1-5d and 1-5i, TR 25-1.
25c. Does the content tell the organization's story to the public?				
25d. What is the impact of the content on the organization's corporate ethos?				

25e. What is the risk to the organization's credibility if publicly released information is omitted and / or deleted from the Web?				
25f. Has information been presented using plain language that considers the knowledge and literacy level of the typical Website visitor?				
25g. Do all HQ TRADOC organizational homepages and subsequent pages follow the template provided by the TRADOC G-6?				
25h. Does the Webpage design for TRADOC subordinate organizations and CoEs / schools make it distinguishable – "branded," with a unique design, corporate identity and clear demarcation – from garrison or other tenant activities at their installations?				
Content-management controls and review procedures				
26a. Does the content comply with DoD Website administration policy, Army Website policy (AR 25-1), Army information-resource management policy (DA PAM 25-1-1), TRADOC regulations, and guidance for official, publicly accessible Websites, and any subsequent policies and guidance memorandums?				
26b. Has PAO notified content providers of "no" responses to AR 25-1, Appendix C-4, test questions and other policy violations?				
26c. Has PAO followed up on the notifications to the content provider and ensured violations were corrected?				

LOSS-OF-PII CONSEQUENCE TABLE

Consequence (Loss of PII may cause the individual to experience these consequences)	Impact *Per OMB M-07-16, loss of PII must be considered at least "moderate" or "high" impact.				
	Insignificant	Low	Moderate*	High*	Catastrophic
Personal injury (bodily)	No injury	Injury but limited adverse effect; individual is treated and released	Bodily injury but not serious or life-threatening; individual is hospitalized	Serious or life-threatening bodily injury	Death or permanent disability
Personal injury (mental pain)	No injury	Suffers emotional distress from disclosure of private facts	Treatment by psychiatrist / psychologist; fear and uncertainty over potential for usage of private facts for blackmail, denial of employment, or harassment due to unwarranted exposure	Debilitated / stressed to point of missing 8 or more hours of work each week	Attempted suicide or suicide; permanent disability
Property loss, including identity theft	No loss	Individual experiences identity theft but financial loss of less than \$500; must re-establish identity with local, state and federal agencies	Loss of property (due to break-in because of release of home address, for instance) or other financial loss (due to identity-theft-related charges to a charge card, for instance), or any other financial loss, to person greater than \$500 but less than \$2,500	Loss of property or financial loss to person greater than \$2,500 but less than \$8,000	Loss of property or financial loss to person greater than \$8,000
Embarrassment or harm to reputation	No embarrassment or harm to individual	Embarrassment or harm to reputation of individual but no lasting adverse affect; individual suffers inconvenience	Moderate embarrassment or harm to individual; individual suffers harassing comments and / or telephone calls; individual suffers mental pain equivalent to moderate impact	Major embarrassment or harm to reputation of individual; individual suffers job demotion or pass-over for promotion; individual suffers mental pain equivalent to high impact	Catastrophic embarrassment or harm to reputation of individual, including irreparable harm; individual suffers job loss or legal repercussions

<p align="center">RELEASABILITY CHECKLIST</p> <p align="center">* Use this checklist to check if an information concern or category is releasable. Key to second column = release yes (Y), no (N) or depends (D) on situation; check reference(s) and refer to conditions/notes.</p>			
Area of concern	Y / N / D	Refer to	Conditions / notes
Criminal and Inspector General (IG) investigations, legal cases, disciplinary actions, and related categories			
Disciplinary actions	D	AR 25-55 for guidance	IAW Paragraph 5-16, AR 360-1.
Coverage of court-martial – --Photos or video of courtroom interior when individuals involved in the proceedings are not present --Photos or video of accused in courtroom, cell, cell block, prison yard or similar area, or in the presence of other prisoners --Photos or video of accused when he / she is outdoors in public view	Y	Paragraphs 5-29 and K-8b, AR 360-1	Court-martial proceedings are public. More restrictive measures, however, may be necessary to ensure a fair trial.
	N		
	Y		
Criminal investigations and DA polygraph activities	D	Paragraph 2-9, AR 195-6, for guidance	IAW Paragraphs 5-17 and 5-45, AR 360-1, and Paragraph 6-7c(4), AR 25-1. Generally, information concerning an ongoing investigation (or the incidents that are part of that investigation) is non-releasable. However, in coordination with local authorities, PAOs may acknowledge the existence of an investigation and release information that is a matter of public record.
Information from criminal investigation and military police records, reports, and forms	D	AR 190-45, AR 195-2, and AR 340-21 for guidance	IAW Paragraph 5-18, AR 360-1.
Litigation	D	Paragraph 5-28a, AR 360-1	To preclude the premature release of information about litigation cases, a close liaison with the SJA concerned must be maintained. As discussed in AR 27-40, Paragraph 7-9, matters in litigation or with the potential for litigation will not be discussed unless the information is a matter of public record. In this case, the PAO and SJA will coordinate responses to queries. PAOs will never speculate on such matters, but will advise the SJA concerned of any media queries regarding cases in litigation.
Debarment cases	D	Paragraph 5-28b, AR 360-1	To preclude the premature release of information about debarment cases, a close liaison with the SJA concerned must be maintained. Information about debarment of a company holding a government contract will not be released until a final decision is made. In the interim, PAOs may acknowledge that a specific company has been proposed for debarment. The media should be referred without comment to the contractor when questions arise about the basis for the case or the status of the proceedings.
Photography in Army confinement facilities	N	Paragraph 10-12, AR 190-47	IAW Paragraph 5-44, AR 360-1.

IG investigations	N	Paragraph 3-5g, AR 20-1	IAW Paragraph 5-46, AR 360-1. IG investigations contain sensitive information and advice. Unauthorized use or release of IG records can seriously compromise the IG's effectiveness as a trusted adviser to the commander and may breach IG confidentiality. This is different from the results of IG audits; the office of the DoD IG routinely releases the results of its audits via its Website.
Character of discharge – punitive	Y	Paragraph K-8b, AR 360-1	In discharges resulting from courts-martial, the proceedings and record are not restricted by the Privacy Act because that act incorporates the definition of agency found in 5 USC 551(1), which specifically excludes court-martial (5 USC 551(1)(F)). Court-martial proceedings are public. Therefore, the approved sentence and subsequent clemency action, if any, are releasable.
Civil disturbances	N	Paragraph 5-47b, AR 360-1	OCPA is responsible for PA activities in connection with civil disturbances. Questions on public-information matters related to civil disturbances will be referred to OCPA by Active Army elements and / or Reserve Component units on active-federal-duty status. Army National Guard units on state active duty will refer questions to the NGB PA.
Casualties, medical condition and treatment, medical records			
Personnel who are or were participating in Army alcohol- and drug-abuse control programs	N	Paragraph 5-27, AR 360-1	
Personnel under treatment in Army medical facilities – in response to query – date patient was admitted to and / or released from the medical facility	Y	Paragraphs 5-25 and 5-32, AR 360-1	Caveat: Information about patients under treatment in Army medical facilities will be released only IAW the FOIA and Privacy Act. PII, other than that releasable under AR 340-21, will not be released without the prior informed written consent of the individual or, if the individual is unable to function for himself / herself, by his / her representative. In addition, the attending physician and / or medical facility commander must determine that photographing or recording activity will not jeopardize the condition or welfare of the patient or nearby patients. Photographing a patient will be prohibited when it infringes on the patient's right to privacy or causes embarrassment. Photographing patients must always meet accepted standards of propriety.
Personnel under treatment in Army medical facilities – in response to query – general information identifying the type of injury or disease	Y	Paragraph 5-25, AR 360-1	E.g., burn, fracture, gunshot wound or pneumonia. Avoid any statement that may invite speculation.
Personnel under treatment in Army medical facilities – in response to query – description of patient's specific condition	D	Paragraph 5-25, AR 360-1	Only with the patient's informed consent; this consent should be in writing.

Personnel under treatment in Army medical facilities – in response to query – current assessment of patient's condition	Y	Paragraph 5-25, AR 360-1	Limit the statement to "The patient's condition is stable (or good, fair, serious, or critical)"; do not give a prognosis under any circumstances.
Photographing and recording personnel in a hostile area	D	Paragraph 5-31, AR 360-1	Use care when releasing official information, photographs, and video recordings of U.S. and allied forces personnel killed, wounded in action, hospitalized, detained as a result of hostile action, or MIA. Give every consideration to the rights of the individuals concerned and the effect publishing information or photographs would have on families and friends.
Photographs or video recordings of recognizable wounded or deceased personnel not identified by name	D	Paragraph 5-31c(1), AR 360-1	Applies while a wounded person is in an area of hostile action, at a point of embarkation or entry, at a hospital or other military convalescent installation, or in transit. If individual shown has given permission to release and a notation is placed at the end of the identifying caption, official release can be made.
Photographs or video recordings of recognizable wounded personnel identified by name	D	Paragraph 5-31c(2), AR 360-1	Conditions above apply. Also, next-of-kin must have been notified (unless the wounded requested his/her NOK not be notified) before release can be made.
Surgical or other major medical care photographs or video recordings that identify the patient	N	Paragraph 5-31c(3), AR 360-1	
Photographs or video recordings showing deceased and/or wounded personnel in large numbers	N	Paragraph 5-31c(4), AR 360-1	Official photographs of combat deceased under field conditions normally will not be released to the public media. Photographing graves registration facilities or temporary cemeteries is prohibited.
Photographs or video recordings showing mangled bodies, obvious expressions of agony, or expressions of severe shock	N	Paragraph 5-31c(5), AR 360-1	
Photographs or video recordings of psychiatric or other mental patients	N	Paragraph 5-31c(6), AR 360-1	
Photographs or video recordings of plastic surgery or severe disfigurement cases	N	Paragraph 5-31c(7), AR 360-1	
Photographs or video recordings of blind or deaf patients	N	Paragraph 5-31c(8), AR 360-1	
Photographs or video recordings of amputees demonstrating prosthetic appliances	N	Paragraph 5-31c(9), AR 360-1	
Casualty information – specifically before verification that next-of-kin have been formally notified by the military service concerned	N	Paragraph 5-20, AR 360-1	
Disclosure of medical records	N	Paragraph 4.7, DoDD 5400.11; Paragraph 6-	Prohibited except as authorized by DoD 6025.18-R [DoD Health Information Privacy Regulation , Jan. 24, 2003].

		7c(4), AR 25-1	Medical records are FOIA-exempt as records which, if released, would result in a clearly unwarranted invasion of personal privacy.
Information or imagery of enemy personnel killed, wounded in action, or hospitalized	N	Paragraphs 5-25b and 5-31, AR 360-1	Treatment of enemy personnel is not specifically considered by AR 360-1, but best practice is to extend the same consideration to enemy KIA, WIA, or hospitalized as to U.S. / Allied personnel.
Casualty information on key U.S. government personnel or equivalent foreign-government personnel	N	Paragraph 5-3a(18), AR 360-1	Releasable only by OSD.
Missing in action			
Missing in action – names and addresses of next-of-kin	N	Paragraph 5-26, AR 360-1	
Missing in action – photographs or video of person MIA	N	Paragraph 5-26, AR 360-1	
Missing in action – MIA's name, grade, and date of birth; statement indicating the MIA's status	Y	Paragraph 5-26, AR 360-1	If PAO has verification that next-of-kin were officially notified and search-and-rescue operations were terminated. DOB cannot be released on the public-domain Web, however.
Missing in action – circumstances of or other details about the release, escape, or other method of return to military control of personnel classified as MIA	Y	Paragraph 5-26, AR 360-1	If PAO has verification that the next-of-kin were officially notified.
Missing in action – data on MIA's physical condition or scheduled return to the United States, or information that former MIAs may provide about other persons known or believed to be casualties or MIA	D	Paragraph 5-26, AR 360-1	If PAO has verification that next-of-kin were officially notified, but there may be OPSEC / security issues involved.
Army and unit structure, status, movement, and training			
Opposing Forces (OPFOR) program	D	Section VI, AR 350-2, for guidance on policy for public displays and / or demonstrations of OPFOR equipment and training.	IAW Paragraph 5-35, AR 360-1. Releasing information about the OPFOR program is restricted.
Activation, inactivation, or realignment of installations, facilities, or activities, and / or associated personnel reductions	Y	Paragraph 5-38a, AR 360-1	Accurate and timely information, consistent with security and the policies of AR 5-10, will be released to the public when the decision has been made to activate, inactivate, or realign an installation, facility or activity, and / or associated personnel reductions. Initial announcement must be made by OCPA.
Unit activation, inactivation, and reorganization	D	Paragraphs 5-3 and 5-39a, AR 360-1	Normally, the initial release of information on activations, inactivations, and reorganizations of Active Army units of brigade or larger size will be made at the national level. This does not apply to announcements of such actions for Reserve Component units. (See AR 5-10.)

Exact personnel strength and composition of units	N	Paragraph 5-39b(1), AR 360-1	This is safeguarded information and is generally not releasable. Applies to any phase of unit activations, inactivations, redesignations, reorganizations, training, or movements within the United States or overseas. Commanders may approve release of information when release will not compromise OPSEC.
Status, amounts, or quality of a unit's equipment	N	Paragraph 5-39b(2), AR 360-1	This is safeguarded information and is generally not releasable. Applies to any phase of unit activations, inactivations, redesignations, reorganizations, training, or movements within the United States or overseas. Commanders may approve release of information when release will not compromise OPSEC.
Combat efficiency of a unit	N	Paragraph 5-39b(3), AR 360-1	This is safeguarded information and is generally not releasable. Applies to any phase of unit activations, inactivations, redesignations, reorganizations, training, or movements within the United States or overseas. Commanders may approve release of information when release will not compromise OPSEC.
Deployment of units to combat areas	N	Paragraph 5-39b(4), AR 360-1	This is safeguarded information and is generally not releasable. Applies to any phase of unit activations, inactivations, redesignations, reorganizations, training, or movements within the United States or overseas. Commanders may approve release of information when release will not compromise OPSEC.
Unit activation, inactivation, redesignation, and reorganization of Reserve Component unit	D	Paragraph 5-39c, AR 360-1	For U.S. Army Reserve units, the local commander may release this information about the local unit: exact personnel strength and composition of unit; status, amounts, or quality of equipment; combat efficiency. For Army National Guard units, the NGB will notify the unit concerned. When this notification is received, the State Adjutant General concerned may release this information about the local unit: exact personnel strength and composition of unit; status, amounts, or quality of equipment; combat efficiency.
Training and movement of units	D	Paragraph 5-40, AR 360-1	Information on unit training or movement that is not safeguarded or restricted by Paragraph 5-4 or other provisions in AR 360-1 may be released by the responsible commander, except in the cases of major or Joint exercises. Initial release of information on major Army exercises will be made at HQ DA, through OSD. Initial release of information on major Joint exercises will be made by OSD, with later announcements by the Joint commander.
Military facilities			
Photography of military installations or equipment	Y	Paragraph 5-33a, AR 360-1	Army installations are generally open to the public. Photographing historical buildings or areas of public interest for private use is

			permitted.
Ground or aerial photographs, sketches or graphic representations of classified military equipment or installations designated as restricted areas	N	Paragraph 5-33b, AR 360-1	Punishable by law (18 USC 795). Reproducing, publishing, or selling this type of material is also punishable by law unless the photograph, sketch, or graphic representation indicates it has been reviewed and cleared for release by proper authority.
Military Entrance Processing Stations	D	Paragraph 3-11, AR 601-270, for guidance	IAW Paragraph 5-41, AR 360-1.
Commissaries	Y	Paragraph 5-42, AR 360-1	Coordinate with the PAO of the Defense Commissary Agency, Fort Lee, Va.
Miscellaneous			
Visual information that does not accurately portray Soldiers in situations reflecting Army activities, missions, and uniforms	N	Paragraph 5-30, AR 360-1	
Army participation in disaster-relief operations	Y	AR 500-60 for PA responsibilities	IAW Paragraph 5-47a(1), AR 360-1. Information on Army participation in disaster-relief operations will be made available promptly.
Information that misrepresents the Army	N		Called a category of "sensitive" information and non-releasable.
Statements in conflict with good order, morale, discipline, and mission accomplishment	N		Called a category of "sensitive" information and non-releasable.
Fundraising publicity – quotas, competition, or tallies	N	Paragraph 13-15a, AR 360-1	Do not release quotas, competition, or tallies of solicitation between or among agencies. Discuss the campaign in general and focus on participation by command personnel, not specific CFC agencies.
Fundraising publicity – information that states, implies or in any way inspires the existence of competition among units, offices, activities, or personnel to raise funds	N	Paragraph 13-15b, AR 360-1	Stories that compare unit participation or progress of subordinate units are prohibited.
Intelligence / counterintelligence personnel and activities			
U.S. Army / DoD counterintelligence personnel or activities	N	Paragraphs 5-3 and 5-24, AR 360-1	Public release of this information must be authorized by INSCOM PAO. This information is restricted.
Records pertaining to National Security Agency, Defense Intelligence Agency, National Reconnaissance Office, and National Geospatial-Intelligence Agency personnel	N	Paragraph 4.7, DoDD 5400.11	Disclosure of records on personnel assigned to these agencies shall be prohibited to the extent authorized by Public Law 86-36 (1959) and 10 U.S.C. 424.
Research and development, testing, and simulations			
Army studies	N	Paragraph 5-34, AR 360-1	Premature release of emerging results of Army studies and/or analyses before official approval is prohibited.

Developmental, technological validation, or operational equipment testing	N	Paragraph 5-36, AR 360-1	Coverage of Army-systems testing is prohibited.
Battle labs and advanced warfighting experiments (AWEs)	Y	Paragraph 5-37, AR 360-1	At ACOM level, and in coordination with OCPA.
Ongoing test or evaluation programs	N	Paragraph 13-2g, AR 360-1	Coverage is prohibited. Seek exceptions to policy through channels to OCPA (see Paragraph 5-36, AR 360-1).
Scientific and technical information	D	Paragraph D-2b, AR 360-1	Scientific and technical information will not be released if it discloses classified military applications, or, if unclassified, disclosure would be adverse to the national interest. DoD or higher authority will release scientific and technical information that would generate national public interest.
Certain technical data	N	DoDI 5230.29	Not releasable if the document contains technical data, including data developed under contract or independently developed and subject to potential control that may be militarily critical and subject to limited distribution, but on which a distribution determination has not been made.
Weapons of mass destruction, other munitions, NBC facilities and accidents / incidents, and nuclear facilities			
Coverage on installations with chemical munitions and/or a nuclear, biological, or chemical defense-related mission or activity	D	Paragraph 5-43, AR 360-1	Coverage of NBC missions or activities is case-by-case basis and approved by the chemical activity or installation commander.
NBC accidents and incidents concerning materials under the supervision or responsibility of the Army	D – specifics follow	Paragraphs 12-1a and 12-3b, AR 360-1	<p>The public is entitled to all unclassified information concerning an accident when AR 360-1 or other directives or instructions allow it. Furnishing this information to the public in a positive manner is in the national interest and is a command function.</p> <p>An incident is not as urgent as an accident; however, an incident may impose a responsibility to inform the public. This determination depends upon the type and scope of the incident and the severity and potential impact the presence of biological and chemical components, materials, or facilities at the incident site may have on the public.</p>
NBC accidents and significant incidents – nuclear	D	Paragraphs 12-1a(1), 12-1b, and 12-4e, AR 360-1	<p>DA policy is that, normally, the presence of nuclear weapons or nuclear components will not be confirmed or denied. However, in the event of a serious accident involving a nuclear weapon, official confirmation of the presence of such weapons may be made when it will have public-safety value; will reduce or prevent widespread public alarm; and will ensure public understanding of the extent and nature of the public hazard resulting from the accident and of the safety precautions being taken.</p> <p>Releasing information about the reactor or nuclear materials which is beyond the scope of this guidance must be approved in advance by OCPA. It is Army policy not to comment on facilities, nuclear materials, or</p>

			<p>matters involving agencies outside DA.</p> <p>Most information on nuclear weapons and their storage is classified as restricted data or formerly restricted data and is very sensitive. Examples include information on the design of nuclear weapons and components, disclosure of whether or not a weapon contains tritium, disclosure of tritium's physical state and chemical form, and data on the specific location of nuclear weapons.</p>
NBC accidents and incidents – biological	Y	Paragraph 12-1a(2), AR 360-1	Unless precluded by valid security concerns, information on a serious incident involving biological weapons or agents will be provided to the public and news media in a timely and accurate manner consistent with requirements. Releasing officials are specified in Paragraph 5-3, AR 360-1.
NBC accidents and incidents – chemical	Y	Paragraph 12-1a(3), AR 360-1	Unless precluded by valid security concerns, information on a serious incident involving chemical weapons or agents will be provided to the public and news media in a timely and accurate manner consistent with requirements.
Initial information on new chemical munitions; NBC defense or related matters; or other weapons or weapons systems. Or significant modifications or improvements to existing weapon systems, equipment, or techniques	N	Paragraphs 5-3 and 12-2, AR 360-1; DoDI 5230.29	Prior to the initial release of information outside DoD, the information will be coordinated with OCPA. This applies to all Army agencies, contractors, subcontractors, vendors, and suppliers. Releasing this type of information may become an item of national interest. Such information must be cleared through OASD(PA) by OCPA.
Routine use of non-chemical surety material, such as pyrotechnics, flamethrowers, smoke agents and delivery means, and incendiaries	Y	Paragraph 12-2e, AR 360-1	
Unclassified chemical agents, items of equipment, or techniques used for training purposes only	Y	Paragraph 12-2e, AR 360-1	
Information on weapons of mass destruction (including nuclear weapons) and the components of such weapons	N	Paragraph 5-3, AR 360-1; DoDI 5230.29	Must be cleared through OASD(PA) by OCPA. Includes nuclear-weapons-effects research; chemical warfare and defensive biological and toxic research; high-energy lasers and particle-beams technology; and NBC defense testing and production, policies, programs, and activities.
Contracts / contracting			
Release of information by manufacturers, research organizations, educational institutions, and other commercial entities holding Army contracts	D – specific exceptions follow	Paragraph 5-48b, AR 360-1	Army policy is to make available to the public the maximum accurate information on Army contractual relationships, industry accomplishments, and scientific achievements. Exceptions to this policy include safeguarded information as well as data that offers unfair and competitive advantages to specific entities and individuals; non-exportable commercial information or data and information subject to International Traffic in Arms Control;

			information about material in the Military Critical Technology List. This list is available in military contracting and research and development offices. PAOs will not release or authorize release of material that contains implied DA endorsement of a commercial firm, product, or service; or comparison of the merits of one item of military material with another.
DoD specification details or results of acceptance tests	N	Paragraph 5-48d, AR 360-1	
Critical military technology	N	Paragraph 5-48d, AR 360-1	
Procurement information	N	Paragraphs D-1b and D-1c, AR 360-1	DA agencies, contractors, or educational institutions will not release procurement information on Army-contracted R&D projects without prior approval and clearance from the Assistant Secretary of the Army (Acquisition, Logistics, and Technology).
Data that offers unfair and competitive advantages to specific entities and individuals	N	Paragraph 5-48b, AR 360-1; Paragraph 6-7c(4), AR 25-1	This type of info is FOIA-exempt. Per AR 25-1, Army organizations using the Internet will not post the following types of information on the Army's public Websites: trade secrets and commercial or financial information obtained from a private source which would cause substantial competitive harm to the source if disclosed.
Non-exportable commercial information or data and information subject to International Traffic in Arms Regulation (ITAR) control	N	Paragraph D-2c, AR 360-1	Export and ITAR restrictions may govern release of certain information. See DoDD 5230.24 and DoDD 5230.25 for guidance in making this determination. Approval from OASD is required for such a release.
Information about material in the Military Critical Technology List	N	Paragraphs 5-3 and 5-48b, AR 360-1; Paragraph 6-7c(4), AR 25-1	This type of info is FOIA-exempt. Per AR 25-1, Army organizations using the Internet will not post the following types of information on the Army's public Websites: information and materials, including submissions by defense contractors, involving critical military technology.
Initial announcement of awarded Army contracts valued at more than \$3 million	N	Paragraph 5-3, AR 360-1	Must be made IAW the applicable provisions of the Federal Acquisition Regulation, Defense Federal Acquisition Regulation Supplement, and Army Federal Acquisition Regulation Supplement.
Information infrastructure			
Information concerning communications security (COMSEC), electronic warfare (EW), signal intelligence (SIGINT), computer security (COMPUSEC), command, control, communications, computers, and intelligence (C4I), and information operations (IO)	N	Paragraph 5-3, AR 360-1; DoDI 5230.29	Must be released by OSD.
Release of information regarding information-system infrastructure architecture	N	Paragraph 4-13a, AR 25-2	All Army personnel and contractors will protect and restrict access to all documentation describing operational IS

			architectures, designs, configurations, vulnerabilities, address listings, or user information. This information is a minimum of FOUO and will not be made publicly accessible. Evaluate FOIA requests for such documents in these categories on a case-by-case basis.
Specific vulnerabilities of a system or network	N	Paragraph 4-13b, AR 25-2	All information or IS responses that document or display specific vulnerabilities of a system or network that would aid attempts by an adversary to compromise those critical systems or networks are OPSEC-sensitive and will be protected, controlled, marked, or stored at the appropriate classification level for the system concerned. This information will not be made publicly available.
Interrelated processes	N	Paragraph 4-13c, AR 25-2	Protect and restrict access to information that is a collection of interrelated processes, systems, and networks that provides information on information-assurance (IA) services throughout the Army, the knowledge-management enterprise, or the incident detection and response infrastructure, capabilities, or configuration. This information should be marked FOUO and may be exempt from mandatory release pursuant to the FOIA. Coordinate with your servicing FOIA or Privacy Act office and servicing judge advocate or legal adviser before releasing or deciding to withhold such information.
Personally identifying information (PII)			
Age	N	Paragraphs 5-15, 9-7, and K-2, AR 360-1	Non-releasable PII (as protected by the Privacy Act). Age information is not routinely or normally releasable. Reasons for disclosure must be evaluated and balanced against the degree of personal privacy invasion.
Date of birth	N	Paragraphs 5-15, 9-7, and K-2, AR 360-1	Non-releasable PII (as protected by the Privacy Act). Date-of-birth information is not routinely or normally releasable. Reasons for disclosure must be evaluated and balanced against the degree of personal privacy invasion.
Social Security Number (SSN)	N	Paragraphs 5-15 and 9-7, AR 360-1; Paragraph 4-3, AR 340-21	Non-releasable PII (as protected by the Privacy Act). Also, Executive Order 9397 authorizes DA to use the SSN as a system to identify Army members and employees. Once a military member or DA civilian employee has disclosed his / her SSN for purposes of establishing personnel, financial, or medical records upon entry into Army service or employment, the SSN becomes his / her identification number. No other use of this number is authorized.
Home address	N	Paragraphs 9-7 and K-3b, AR 360-1	Non-releasable PII (as protected by the Privacy Act). Usually, in response to questions, an individual's present location – for example, Clinton, Md. – may be

			provided but not the individual's street address.
Duty address	D	Section 505.7, 32 CFR, The Army Privacy Program	Per cited reference et al, no release of duty addresses of DoD military members and civilian employees, especially duty addresses for units that are sensitive, routinely deployed, or stationed in a foreign territory (see below). IAW AR 340-21, compilations of unit / office addresses of military personnel may not released when the requester's main purpose in seeking the information is to use it for commercial solicitation. However, military personnel's duty address is not exempt from required release under the FOIA and therefore must be released to the public if requested.
Home telephone number	N	Paragraphs 5-15 and 9-7, AR 360-1	Non-releasable PII (as protected by the Privacy Act).
Duty phone number	D	Paragraph 6-7c(4)(i), AR 25-1	POC contact information in posted memoranda may include office telephone number. However, IAW AR 340-21, compilations of unit / office telephone numbers of military personnel may not released when the requester's main purpose in seeking the information is to use it for commercial solicitation. Military personnel's duty phone numbers and federal civilian employees' office or duty phone numbers are not exempt from required release under the FOIA and therefore must be released to the public if requested.
Marital status	N	Paragraphs 5-15, 9-7, and K-4, AR 360-1	Non-releasable PII (as protected by the Privacy Act). An individual's marriage status is not routinely or normally disclosed. Reasons for disclosure must be evaluated and balanced against the degree of personal privacy invasion.
Family members' names	N	Paragraphs 5-15, 9-7, and K-4, AR 360-1	Non-releasable PII (as protected by the Privacy Act). Is part of individual's marital status.
Family members' sexes	N	Paragraphs 5-15, 9-7, and K-4, AR 360-1	Non-releasable PII (as protected by the Privacy Act). Is part of individual's marital status.
Family members' SSNs	N	Paragraphs 5-15 and 9-7, AR 360-1; Paragraph 4-3, AR 340-21	Non-releasable PII (as protected by the Privacy Act).
Race / ethnic origin	D	Paragraphs 5-15, 9-7, and K-7, AR 360-1	Non-releasable PII (as protected by the Privacy Act). However, a specific request may be made under circumstances where it is relevant; for example, a racially oriented protest or altercation. When an individual's race is relevant to the essential facts, it may be released.
Civilian-education degree(s) and major area of study	D	Paragraphs 5-15, 9-7, and K-6, AR 360-1	Listed as non-releasable PII (as protected by the Privacy Act), but generally releasable under the FOIA.

School and year of graduation	D	Paragraphs 5-15, 9-7, and K-6, AR 360-1	Listed as non-releasable PII (as protected by the Privacy Act), but generally releasable under the FOIA.
Educational level; specialty designator	D	Paragraphs 5-15, 9-7, and K-6, AR 360-1	Listed as non-releasable PII (as protected by the Privacy Act), but generally releasable under the FOIA. Further, since it is not exempt from required release under the FOIA, a military person's civilian-education level must be released to the public if requested.
Home of record	D	Paragraphs 5-15, 9-7, and K-3, AR 360-1	<p>Listed as non-releasable PII (as protected by the Privacy Act). Under the FOIA, no general rule exists for disclosing an individual's home of record because of the different circumstances present when requests for this information are made, and therefore, requests are weighed on a case-by-case basis. Under the FOIA, the home of record may usually be released if no street address is given. Home-of-record information is ordinarily not releasable under AR 530-1 (may present OPSEC risk) on the public-domain Web, and if information is not releasable on the Web, it is not releasable in any public venue.</p> <p>In addition to considering the Privacy Act, the FOIA, and OPSEC, consider the individual's desire or that of the individual's next-of-kin in disclosing the home-of-record or present geographic location. However, the individual's consent or the individual's next-of-kin's desires do not necessarily control the decision to release. This decision must be balanced against security considerations. On the other hand, if an objection to release is made, a balancing of interests under the FOIA may still require disclosure.</p>
Awards and decorations / citations	Y	Paragraph K-5, AR 360-1	Award and decoration / citation information is releasable. An award, decoration and / or other proper citation presentation is generally a public event. For most awards and decorations, there is a visible token to be worn on the uniform. Further, military personnel's awards and decorations are not exempt from required release under the FOIA (this information must be released to the public if requested).
Character of discharge – administrative	N	Paragraph K-8a, AR 360-1	The character of discharges resulting from administrative processing is not a matter of public record. Do not release any indication of whether or not a discharge is honorable, general or under other-than-honorable conditions. The release of this information to the general public is viewed as an unwarranted invasion of personal privacy and not releasable under the Privacy Act unless the individual provides his or her written consent.
Duty status	Y	Paragraph K-9, AR 360-1	Releasing information such as the fact of unauthorized absence or desertion, hospitalization, in hands of civil authorities

			awaiting trial, and confinement by military authorities awaiting trial is permitted. Military personnel's duty status at any given time is not exempt from required release under the FOIA and must be released to the public if requested.
Personnel-board decisions	D	Paragraph K-10, AR 360-1	Personnel-board decision information is releasable after decision by final approving authority if the board action applies to a category of persons as opposed to an individual; otherwise, it is not releasable. Results of personnel-board actions affecting groups, such as promotion boards and augmentation boards, are releasable. The results of personnel-board actions affecting individuals, such as administrative discharge boards and aviator flight boards, are not generally releasable. The results of the latter category of boards traditionally have not been released. The board proceedings are not public, and the nature of the action taken, often adverse, warrants preservation of its confidentiality. Information that has become a matter of public knowledge through the action of the individual or his / her counsel may be confirmed.
DoD photographs	Y	Paragraph K-11, AR 360-1	Photographs of DoD military and civilian personnel taken for official purposes are generally releasable unless matters are depicted that would constitute a clearly unwarranted personal privacy invasion if disclosed to public view. Generally, award ceremony photographs, official selection file photographs, chain-of-command photographs, and similar photographs are releasable.
Name – single (individual's name)	D	Memorandum from OSD, "Withholding of Personally Identifying Information Under the Freedom of Information Act (FOIA)," Nov. 9, 2001; memorandum from ASD-C3I, "Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites," Dec. 28, 2001; TRADOC Command Guidance: Noble Eagle #02-019, "Personal Data on Unclassified Websites," March 13, 2002; Paragraph 6-7c(4)(i), AR 25-1; Section 505.7, 32 CFR, The Army Privacy Program	In general, an individual's name is not releasable on the public Web, but there are four exceptions to this: 1) name and duty information may be posted of personnel, who by the nature of their position and duties, frequently interact with the public (official, designated command spokespersons); 2) name and duty information of any GO / SES (IAW AR 25-55, Paragraph 3-200, under exemption No. 6, the names of general officers (or civilian equivalent) may be released at any time); 3) name, rank, and duty station of military personnel in photo captions and news stories; and 4) POC information on posted memoranda. Organizations required to post public contact information should use organizational designation / title and generic position email addresses, such as office@organization.mil . On the other hand, names of either military personnel or federal civilian employees are not exempt from required release under the FOIA and therefore must be released to the public if requested.
Name – list	N	Memorandum from ASD-C3I, "Removal of	Lists of names of any personnel assigned to any component, unit, organization, or office

		<p>Personally Identifying Information of DoD Personnel from Unclassified Websites," Dec. 28, 2001; TRADOC Command Guidance: Noble Eagle #02-019, "Personal Data on Unclassified Websites," March 13, 2002; Section 505.7, 32 CFR, The Army Privacy Program; Paragraphs 6-4r(1), 6-4r(2), and 6-7c(4)(i), AR 25-1</p>	<p>within DA are prohibited. Rosters, directories (including telephone directories), and detailed organizational charts showing personnel are considered lists of PII and are prohibited. Multiple names of individuals from different organizations / locations listed on the same document or Webpage constitutes a list.</p> <p>Organizational directories made available to the public will list position titles rather than individuals' names. Electronic versions of organizational directories may be placed on that organizational community page on AKO or AKO-Secure, but not on the publicly accessible Web.</p> <p>Release of emergency-recall rosters should only be shared with those who have an "official need to know" the information, and they should be marked FOUO.</p>
Present or past position titles	N	<p>Section 505.7, 32 CFR, The Army Privacy Program; Paragraph 6-7c(4)(i), AR 25-1</p>	<p>In general, DoD requires that its components not release present or past position titles of DoD military members and civilian employees. POC contact information in posted memoranda may include official title. However, present and past position titles for federal civilian employees are not exempt from required release under the FOIA and therefore must be released to the public if requested. Disclosure of this information, however, may not be made when the FOIA request is a list of present or past position titles, grades, salaries, and / or duty stations and 1) is selected to constitute a clearly unwarranted invasion of personal privacy (for example, the nature of the request calls for a response that would reveal more about the employee than the items listed above); or 2) would be protected from mandatory disclosure under a FOIA exemption.</p>
Present or past duty stations / organizations	N	<p>Paragraph 3-3b(1), AR 340-21; Section 505.7, 32 CFR, The Army Privacy Program</p>	<p>As with other categories, in general, DoD requires that its components not release this type of information about DoD military members and civilian employees. POC contact information in posted memoranda may include organization name, per AR 25-1; no other information, including room numbers, is to be included about POCs.</p> <p>Office / unit name for military personnel and present / past duty stations for federal civilian employees are not exempt from required release under the FOIA and therefore must be released to the public if requested. Disclosure of this information, however, may not be made when the FOIA request is a list of present or past position titles, grades, salaries, and / or duty stations and 1) is selected to constitute a clearly unwarranted invasion of personal privacy (for example, the nature of the request calls for a response that would reveal more about the employee than the items listed above); or 2) would be protected from mandatory disclosure under a FOIA</p>

			exemption.
Position descriptions and identification of job elements for federal civilian employees	Y	Paragraph 3-3b(1), AR 340-21; Section 505.7, 32 CFR, The Army Privacy Program	This category is not exempt from required release under the FOIA and therefore must be released to the public if requested,
Civilian grades and salaries; military rank and pay	D	Section 505.7, 32 CFR, The Army Privacy Program ; Paragraph 3-3a(1), AR 340-21	In general, DoD requires that its components not release grades and salaries of DoD military members and civilian employees. However, the following categories are not exempt from required release under the FOIA and therefore must be released to the public if requested: for military personnel – rank and gross salary; for federal civilian employees – occupational series and grade; present and past annual-salary rates (including performance awards or bonuses, incentive awards, merit-pay amount, meritorious or distinguished executive ranks, and allowances and differentials). (Disclosure of this information, however, may not be made when the FOIA request is a list of present or past position titles, grades, salaries, and / or duty stations and 1) is selected to constitute a clearly unwarranted invasion of personal privacy (for example, the nature of the request calls for a response that would reveal more about the employee than the items listed above); or 2) would be protected from mandatory disclosure under a FOIA exemption.)
Performance standards	D	Section 505.7, 32 CFR, The Army Privacy Program ; Paragraph 3-3b(1), AR 340-21	In general, DoD requires that its components not release performance standards of DoD military members and civilian employees. However, federal civilian employees' performance standards (but not actual performance appraisals) are not exempt from required release under the FOIA and therefore must be released to the public if the release will not interfere with law-enforcement programs or severely inhibit agency effectiveness. Performance elements and standards (or work expectations) may be withheld when they are so intertwined with performance appraisals that the disclosure would reveal an individual's performance appraisal.
Source of commission – military personnel	Y	Paragraph 3-3a(1), AR 340-21; Section 505.7, 32 CFR, The Army Privacy Program	Not exempt from required release under the FOIA and must be released to the public if requested.
Date of rank / promotion sequence number – military personnel	Y	Paragraph 3-3a(1), AR 340-21; Section 505.7, 32 CFR, The Army Privacy Program	Not exempt from required release under the FOIA and must be released to the public if requested.
Professional military education – military personnel	Y	Paragraph 3-3a(1), AR 340-21; Section 505.7, 32 CFR, The Army Privacy Program	Not exempt from required release under the FOIA and must be released to the public if requested.
Separation or retirement dates – military	Y	Paragraph 3-3a(1), AR	Not exempt from required release under the

personnel		340-21; Section 505.7, 32 CFR, The Army Privacy Program	FOIA and must be released to the public if requested.
Military occupational specialty (MOS) – military personnel	Y	Paragraph 3-3a(1), AR 340-21; Section 505.7, 32 CFR, The Army Privacy Program	Not exempt from required release under the FOIA and must be released to the public if requested.
Active-duty official attendance at technical, scientific, or professional meetings – military personnel	Y	Paragraph 3-3a(1), AR 340-21; Section 505.7, 32 CFR, The Army Privacy Program	Not exempt from required release under the FOIA and must be released to the public if requested.
Biographies and photos of key military personnel	Y	Paragraph 3-3a(1), AR 340-21; Section 505.7, 32 CFR, The Army Privacy Program	Not exempt from required release under the FOIA and must be released to the public if requested. OPSEC review must be done and must consider aggregation of key-leader names across Webpages.
Overseas assignments (present or future)	N	Paragraphs 9-7 and K-12, AR 360-1	Listed as non-releasable PII (as protected by the Privacy Act). Name of service member assigned to a unit stationed in a foreign territory is routinely not releasable. Release only if requested under the FOIA, as military personnel's present and past duty assignments, as well as future assignments that are officially established, are not considered exempt under the FOIA and must be released to the public if requested.
Overseas office or unit mailing address	N	Paragraphs 5-3, 9-7, and K-12, AR 360-1	Non-releasable PII (as protected by the Privacy Act). Duty address of military personnel assigned to a unit that is stationed in a foreign territory is not routinely releasable.
Names of military personnel in sensitive or routinely deployed units, or assigned to units stationed in a foreign territory	N	Paragraphs 5-3, 9-7, and K-12, AR 360-1; Paragraph 4.7, DoDD 5400.11	IAW DoDD 5400.11, disclosure of records pertaining to personnel of overseas, sensitive, or routinely deployable units shall be prohibited to the extent authorized by Section 130b of Title 10, U.S. Code. IAW AR 360-1, information of this type may be released only by HQ DA or OASD(PA). The Secretary of Defense (Public Affairs) is the sole approving authority for releasing rosters that list members of this type of unit by name.
Duty phone of routinely deployable or sensitive units	N	Paragraphs 5-3 and 9-7, AR 360-1	See above.
PII that would otherwise be protected from mandatory disclosure under a FOIA exemption	N	Paragraph 9-7, AR 360-1; Paragraph 6-7c(4), AR 25-1	Much of the prohibited information listed in AR 25-1 is FOIA-exempt information. Per AR 25-1, Army organizations using the Internet will not post on the Army's public Websites records which, if released, would result in a clearly unwarranted invasion of personal privacy.
For Official Use Only (FOUO) information			
FOUO (FOIA exempted)	N	Paragraph 6-7c(4), AR 25-1	Generally not releasable.

Records related solely to internal personnel rules and practices that are not meant for public release	N	Paragraph 6-7c(4), AR 25-1	FOIA exempt.
Restricted- or limited-distribution information	N	Paragraph 6-7c(4), AR 25-1	FOIA exempt.
Records protected by another law that specifically exempts the information from public release	N	Paragraph 6-7c(4), AR 25-1	FOIA exempt. Includes information protected by copyright.
Internal records that are deliberative in nature and are part of the decision-making process that contain opinions and recommendations	N	Paragraph 6-7c(4), AR 25-1	FOIA exempt. This exemption includes draft documents, draft publications, or pre-decisional information of any kind.
VIP travel	N	Paragraph 10-6, AR 360-1	General information on VIP travel will be handled as FOUO information. Specific information on VIP travel should be classified (level: confidential) for security reasons.
"Sensitive" or security-related topics			
Classified information	N	AR 380-5	
Information or imagery of U.S. coalition forces	N	Paragraph 5-31, AR 360-1	Not without an official release signed by the individuals in advance.
Photographs containing sensitive images	N	Paragraphs 2-1c and 2-19, AR 530-1; ALARACT 156/2005, "Chief of Staff of the Army OPSEC Guidance," Aug. 23, 2005; ALARACT, "Sensitive Photos," Feb. 14, 2005	Especially photos showing the results of IED strikes, battle scenes, casualties, and destroyed or damaged equipment.
Information discusses and may affect the OPSEC of IEDs	N	Enclosure 3, DoDI 5230.29	Must be submitted to DoD's Office of Security Review (OSR) for review and clearance.
Information discusses and may affect the OPSEC of initial fixed weapons basing and arms-control treaty implementation	N	Enclosure 3, DoDI 5230.29	Must be submitted to OSR.
Information that affects national security policy, foreign relations, or ongoing negotiations	N	Enclosure 3, DoDI 5230.29	Must be submitted to OSR.
Information that is presented by a DoD employee, who, by virtue of rank, position or expertise, would be considered an official DoD spokesperson	N	Enclosure 3, DoDI 5230.29	Must be submitted to OSR.
Information that originates from or is proposed for release at the seat of government	N	Enclosure 3, DoDI 5230.29; Paragraph 5-3, AR 360-1	Must be submitted to OSR. DoDI 5230.29 adds "by senior personnel on sensitive political or military topics."
Information that is or has the potential to become an item of national or international interest	N	Enclosure 3, DoDI 5230.29; Paragraph 5-3, AR 360-1	Must be submitted to OSR.

Information and public statements with foreign-policy or foreign-relations implications	N	Enclosure 3, DoDI 5230.29; Paragraph 5-3, AR 360-1	Must be submitted to OSR.
Information on subjects of potential controversy among the military services or with other federal agencies	N	Enclosure 3, DoDI 5230.29; Paragraph 5-3, AR 360-1	Must be submitted to OSR.
Information on significant military operations, potential operations, OPSEC, and military exercises	N	Enclosure 3, DoDI 5230.29; Paragraph 5-3, AR 360-1	Must be submitted to OSR.
Information on military applications in space	N	Enclosure 3, DoDI 5230.29; Paragraph 5-3, AR 360-1	Must be submitted to OSR.
Information and public statements concerning high-level military or DoD policy	N	Paragraph 5-3, AR 360-1	Must be cleared at HQ DA or above.
Information concerning U.S. government policy or policy within the purview of other government agencies	N	Paragraph 5-3, AR 360-1	Must be cleared at HQ DA or above.
Information on national command authorities (NCAs) and NCA command posts	N	Paragraph 5-3, AR 360-1	Must be cleared at HQ DA or above.
Initial announcement of GO assignments	N	Paragraph 5-3, AR 360-1	Must be cleared at HQ DA or above.

Chapter 4

Web-content managers / Web-content management

The previous chapter discussed PAO's role as the uber-reviewer, which naturally moves into the uber Web-content manager. We touched on the subject in Chapter 1, but this chapter discusses Web-content planning and oversight in more detail. There are many "moving pieces and parts" to being a true Web-content manager, but it boils down to what to do and what to be aware of – which this chapter's sections discuss.

ORGANIZATIONAL WEBSITE COORDINATOR

Although overall Web-content manager, PAO needs management teammates. First, PAOs should set the conditions (such as convince the boss and write the local SOP) that the local content-review process requires the command's organizations to appoint a Website coordinator – who is the person the overall Web-content manager looks to for management and coordination of his / her organization's Web products. The Website coordinator also fields a number of the questions from his / her organization's members that would ordinarily be directed to PAO or G-6.

Although industry uses the term in various ways, a **Website coordinator**, as referred to in Chapter 3, is essentially the **Web-content manager on an organizational level**. He / she ordinarily has the **following responsibilities**:

- Provide overall management of organizational (e.g., DCG-, DCS-, division-, directorate-, or branch-level) Websites;
- Establish the Website as a core business function IAW its core competencies for the organization, focusing on the Website as a value-added information product for "customers" such as organizational users as well as Army and general-public users;
- Ensure the Website is in compliance with federal, DoD, Army, and TRADOC Web policy;
- Periodically (at least quarterly) review *all* the organization's posted content, including monitoring content (including links) for currency, accuracy, and policy alignment; checking for broken links or content errors; and updating contact phone numbers and e-mail addresses;
- Assist his / her organization's staff with development of Web products and coordinate with TRADOC PAO on the same;
- Keep TRADOC PAO up-to-date on organizational-level Web projects;
- Monitor the content provider's progress through the review process and / or coordinate the review and approval of content to be placed on Web products;
- Strategically plan and evaluate the organization's Web content for improvement to establish / maintain a robust, relevant, up-to-date Website that ties in with its higher headquarters' strategic-communication topics while remaining the go-to Website for news and information specifically about the organization;
- Work with organizational staff to identify gaps in current Website content and develop content to fill those gaps;
- Archive outdated organizational Web products;
- Design and conduct on-line user-satisfaction surveys on behalf of the commander / director IAW Paragraph 8-2g, DA PAM 25-1-1;
- Represent his / her organization at WCWG meetings or forums on Web issues; and
- Apply best practices in writing for the Web or apply QI standards to reviewing content providers' writing for the Web.

When members of the organization are planning a new Website, the Website coordinator should coordinate with TRADOC PAO and TRADOC G-6. The purpose of this coordination would be to determine Website objectives and target audience; Web publishing destination (e.g., public, controlled access, intranet, or classified server); design, content, and technical requirements; roles and responsibilities; and a tentative schedule for posting.

The Website coordinator should also coordinate review of materials by the organization's OPSEC officer, and the OPSEC officer should notify the Website coordinator if any modifications are recommended as a result of the OPSEC review. Website coordinators should be almost as familiar with the rules governing FOUO information and the aspects of the organization's operations considered critical as the organizational OPSEC officer, since – although the content provider shares primary OPSEC responsibility with the organizational OPSEC officer – the Website

coordinator must monitor this. Also to be assessed is a specific risk to the Army's credibility if publicly released information is omitted and / or deleted from the Web – this is determined by PAO as the overall Web-content manager, in conference with the content provider and Website coordinator.

While it is the commander's / director's ultimate responsibility, the Website coordinator will assist in ensuring that 1) an annual survey of Website users is conducted to assess satisfaction with the Website, and 2) an organization-wide Web-content review to assess valid mission need and accuracy is conducted each year. Each Webpage / organizational Website requires review. Once a review is complete, the Website coordinator reflects completion with an updated date stamp on the page (see content requirements section later in this chapter). Although formal reviews must be conducted yearly IAW policy, all Web content should be reviewed and updated as often as appropriate. See Appendix O for tips on measuring your Website.

POST OR ACOM WEB-CONTENT MANAGER

With fingers in all pies is the overall Web-content manager. Somebody must manage or be in charge of content who is able to see the overall picture as well as who is an SME in communication. Web-content managers check for everything, as you undoubtedly saw via the PAO content reviewer's checklist. (We suggest that you use the PAO content reviewer's checklist in conjunction with the Website coordinator's / Web-content manager's checklist at the end of this chapter.)

There is no such thing as laissez faire Web-content management – Web-content managers must be hands-on and active. Web-content managers must be security conscious. Web-content managers should maintain constant dialogue with their senior leaders. And yes, by DoD policy, the commander / director is ultimately responsible for the Website, but the Web-content manager actually does the work and is a stakeholder as well as an SME.

The Web-content manager at HQ TRADOC is TRADOC PAO. The Web-content manager at installation level should be the TRADOC senior commander's PAO – and is indeed appointed thus by TR 25-1. As we'll look at in the "strategic Webbing" section of this chapter, it's a role that requires viewing the Web strategically (what should be there) as well as from the perspective of the reviewer (which concentrates more on what shouldn't be there). And unlike the conceptual framework of AR 25-1 (see Chapter 1), the Website must be managed from the standpoint of what should be there: e.g., what is valuable, what is relevant, what is legally required, what will hurt corporate ethos if it's not there.

Typical Web-content manager responsibilities are:²⁹⁵

- Prior to posting, approve for release new content posted on the corporate Website, organizational portal, and to AKO unrestricted-content areas.²⁹⁶ New content includes new Websites, new Webpages, and documents posted to Websites, and major updates of Websites. PAO is the commander's designated review and approval authority for the release of official information to the public.²⁹⁷ Publicly accessible, non-restricted Army Websites may only provide information that has been properly cleared for release,²⁹⁸ so PAO must ensure that the information posted to these publicly accessible sites is consistent with federal, DoD, Army, TRADOC, and local command policies.

"[A] lead agency should be appointed to coordinate the on-line 'information lane,' and all other agencies should defer to the lead agency for posting comprehensive government information on that topic. This will reduce duplication, save money, and help consumers find accurate information." – *Putting Citizens First: Transforming On-line Government*, Federal Web Managers Council whitepaper

"Someone at the top has to say, 'The Web is a product and needs to have certain controls, the same as if you were printing a book.'" – Lisa Welchman, founder and principal consultant of Welchman Consulting in Baltimore, quoted in "A Tangled Web We Weaved," *Government Computer News*, April 2, 2007

²⁹⁵ See Paragraph 1-5d, TR 25-1.

²⁹⁶ Paragraph 2-3a(15), AR 530-1; Paragraph 6-7c(3), AR 25-1; Paragraphs 4-5a(7) and 4-20g(11), AR 25-2; Paragraphs 1-5d, 1-5i, 5-3a(4)(c) and 5-5c(1), TR 25-1.

²⁹⁷ Expected to be clearly stated thus in Paragraph 2-4m of the soon-to-be-published AR 360-1.

²⁹⁸ Paragraph 1a, memorandum from DISC4 (now known as the Army's CIO/G-6), "Guidance for Management of Publicly Accessible U.S. Army Websites," Nov. 30, 1998; Paragraph E-9, AR 380-5. See also Paragraph 6-7c(3), AR 25-1.

- In conjunction with the command's CIO / G-6, provide oversight and control of the content on public Websites. Ensure a command public Web program is operated and maintained as the official primary point of access to the command's information on the Internet IAW DoD Web policy and coordinated with Web-management procedures from the command's CIO / G-6. (TRADOC PAO serves as Web-content manager for the TRADOC corporate Website.²⁹⁹ The TRADOC senior commander's PAO is the MSO / CoE Web-content manager.³⁰⁰) Develop and organize content while promoting a consistent look and feel on all TRADOC Web products. Also in conjunction with CIO / G-6, recommend and interpret federal, DoD, DA, and TRADOC Web-content policies. Ensure that Websites are maintained in compliance with relevant policies listed in DoDI 5400.13: Joint Public Affairs Support Element (JPASE)'s CONOPS, May 30, 2006; the DoD Web policy; the DEPSECDEF's memo on Interactive Internet Activity (IIA), June 8, 2007; the DEPSECDEF's memo on "Trans Regional Web Policy," Aug. 3, 2007; OMB Memorandum 05-04, "Policies for Federal Agency Public Websites," Dec. 17, 2004; DoDD 5230.9, "Clearance of DoD Information for Public Release," [Aug. 22, 2008]; DoDD 8500.01E, "Information Assurance (IA)," Oct. 24, 2002; and DoDI 8500.2, "Information Assurance (IA) Implementation," Feb. 6, 2003.³⁰¹
- Maintain ACOM-, MSO-, or CoE-level content and monitor the maintenance of DCG- and DCS-level (or equivalent at MSO / CoE) content – i.e., the "flagship," or the most visible and visited content.
- Conduct quarterly Web content reviews (post-dissemination of information) of public Webpages³⁰² and AKO unrestricted-content areas. Also conduct on-the-spot checks of subordinate-organization Webpages.
- Coordinate the corporate information content, and determine the major communication themes on the homepage and pages linked off the homepage.³⁰³ Assess the risk to the command's credibility if publicly released information is omitted and / or deleted from the Web.³⁰⁴
- Advise on design of the Website, its business-practice needs, and the functions the organization wants to make available.
- Research and develop long-term and annual strategies, goals, and objectives for ACOM / MSO / CoE Web products, as well as establishing procedures and standards for Web products.
- Manage Web marketing, outreach, and messaging efforts IAW "strategic Webbing" concepts outlined later in this chapter.
- Coordinate with the CIO / G-6 on any content that may affect the supporting IT or conformance with Website policies.³⁰⁵
- Ensure Web-content providers have followed the content-approval process, including coordination with the organization's OPSEC officer / security manager, and, if needed, the SJA.³⁰⁶ The TRADOC senior commander's PAO should establish local procedures, in compliance with TR 25-1 – and in coordination with the mission Webmaster, mission portal administrator, OPSEC officer, SJA, and G-2 – for review and clearance of information posted to the command / activity's Websites. At minimum, procedures should include insurance that content providers have coordinated with the local OPSEC officer, local security reviewer, QI Program POC and, if needed, SJA for review prior to disseminating information. As Web-content manager, TRADOC PAO also consults SMEs before clearing information, such as:
 - TRADOC PAO may consult the TRADOC OPSEC officer (TRADOC G-3/5/7), TRADOC G-2 (due to G-2's role as the command security manager), or TRADOC SJA for information reviews and guidance, either before PAO gives approval for posting information or while PAO is performing quarterly Website reviews once information is posted.³⁰⁷

²⁹⁹ Paragraph 2-9b, AR 25-1; Paragraph 1-5d(2) and 1-5i(2), TR 25-1.

³⁰⁰ Paragraph 1-5i(2), TR 25-1.

³⁰¹ Paragraph 6b, Enclosure 2, DoDI 5400.13.

³⁰² Paragraph 6-7c(4), AR 25-1; Paragraph 8-4a, DA PAM 25-1-1; Paragraph 6b(8), TRADOC OPSEC Plan.

³⁰³ Paragraphs 1-5d(1) and 1-5i(4), TR 25-1.

³⁰⁴ See Paragraphs 5.2.2, Part I, and 3.5.2.2, Part II, DoD Web policy. Public Affairs makes the final determination on the "absolute credibility" of defense information released to the public through publicly accessible Websites, but content providers should provide input.

³⁰⁵ Paragraph 1-5d(3), TR 25-1.

³⁰⁶ Paragraphs 1-5i and 5-5c(1), TR 25-1.

³⁰⁷ Paragraph 5-5c, TR 25-1.

- In addition to organizational QI measures, TRADOC PAO consults, as needed / requested, the TRADOC Section 508 SME in the Equal Employment Opportunity Office (EEOO), and coordinates with TRADOC G-6 on FOIA concerns before approving release of information on the publicly accessible Web.
- Provide general staff supervision and approval for the release of VI products to the public.³⁰⁸
- Chair the WCWG. Serve on the TRADOC / MSO / CoE WWG and OWG. Provide direction, guidance, and training for content providers, content reviewers, and Website coordinators via telephone, email, or the WCWG and WCWG portal.
- Maintain written records of reviews and violation notifications, IAW local G-6 / DOIM guidance, based on DA PAM 25-1-1, Paragraph 7-7j, as well as AR 380-5, Paragraphs 1-13 and 4-15b.
- Execute IA responsibilities as required by ARs 25-2 and 25-1; Public Affairs assists in the Army Information Assurance Program (AIAP).³⁰⁹ Public Affairs' IA responsibilities are also mentioned in Chapter 5, AR 25-1, and include Web risk assessment.

"Agencies communicate with citizens via many different 'delivery channels,' including Web, email, publications, live chats, blogs, podcasts, videos, wikis, virtual on-line worlds, and more. But it's difficult to ensure timeliness and consistency when various delivery channels are managed by different divisions within an agency. Agencies should provide multiple ways for people to contact them and ensure that information is consistent across all channels. They should be funded to coordinate all types of content targeted to the general public (Web, publications, call center, email, common questions, Web chat, etc). Agencies should be rewarded for delivering consistent information, both within agencies and across government." – **Putting Citizens First: Transforming On-line Government**, Federal Web Managers Council whitepaper

More broadly, Web-content manager functions are established by DoDD 5122.5 and its "companion," DoDI 5400.13. Although the DoDD is specific to the Assistant SECDEF for Public Affairs (ASD-PA), lower-level PAO functions should parallel DoD Public Affairs' organization and functions as much as possible:

- **Adviser to the commander** – "[Public Affairs] is the adviser ... for news-media relations, public liaison, internal communications, community relations, public affairs and [VI] training, and audiovisual matters."³¹⁰
- **Primary communicator** – Public Affairs is called "a **primary DoD communications capability**" in the DEPSECDEF memorandum, "2006 Quadrennial Defense Review (QDR) Strategic Communication (SC) Execution Roadmap."³¹¹ "[Public Affairs] activities shall ... [communicate] information about military activities to domestic, international, and internal audiences."³¹² "[Public Affairs] activities' capabilities shall be developed and employed to support the command's operations to assure the trust and confidence of the U.S. population, friends and allies; deter and dissuade adversaries; and counter misinformation and disinformation, ensuring effective, culturally appropriate information delivery in regional languages according to [DoDI] 5160.70."³¹³
- **Strategic planner and policy-maker** – "[Public Affairs] will develop communications policies, plans, and programs in support of DoD [Internet] objectives and operations in coordination with the Assistant Secretary of Defense for Networks and Information Integration (ASD-NII) / DoD CIO as appropriate."³¹⁴ "[Public Affairs] will establish a communication,

³⁰⁸ Parallels Paragraph 2-9a, AR 25-1.

³⁰⁹ Paragraph 3-3j, AR 25-2. Also see Paragraph 4-5a(7), AR 25-2: "[U]sers are not to release [or] disclose ... information without the consent of ... the Public Affairs Office. ..."

³¹⁰ Paragraph 3, DoDD 5122.5.

³¹¹ Paragraph 1b, DoDI 5400.13.

³¹² Paragraph 4a, DoDI 5400.13.

³¹³ Paragraph 4b, DoDI 5400.13.

³¹⁴ Paragraph 3c, DoDD 5122.05. See also Paragraph 1d, Enclosure 2, DoDI 5400.13.

integration, and planning activity focusing on mid- to long-range strategic communication planning, and issues, trends, and objectives of broad scope and importance to DoD components.”³¹⁵

- **Public Web program manager** – “[Public Affairs] will ensure a consolidated ... [p]ublic Web [p]rogram is operated and maintained as the official primary point of access to DoD information on the Internet [IAW] Website policies and procedures established by [CIO], [and will] serve as the approval authority for ... [IIA]. ...”³¹⁶ Further, according to Army regulations: “All commanders will resource and maintain a [Public Affairs] capability to **operate on the Internet** and to **monitor the global information environment**.”³¹⁷

The Web is a large provider of information to most, if not all, target audiences; DoD realizes this and charges the secretaries of the military departments (MILDEPs) to ensure that Public Affairs has capability sufficient to “conduct and interface with the technologies employed by target populations ... for all planned and ongoing Public Affairs activities.”³¹⁸ While this may be seen as permission to conduct social-networking activities as a primary means of employing technologies already used by target populations that other means cannot reach, operating in the social-media “battlespace” is problematic, as will be discussed further later in this chapter.

The Web-content manager must ensure that content not only feeds the information needs of the taxpayers who are actually funding the Website, but also is relevant to the internal audience. AR 360-1 states that “[t]he primary function of Army electronic media is to support a commander’s internal-information objectives,”³¹⁹ which somewhat clashes with other Army policy that electronic media must be of value to the American public at large. TRADOC PAO agrees that one function of Army electronic media is to support internal-information programs, but that’s not its primary function. Electronic media should 1) provide both Army-wide and local information; 2) assist the commander in identifying and correcting command problems; and 3) act as tools for two-way communication. Internet editorial and news policies must also support the commander’s responsibility to keep the command informed, so PAOs are responsible for deliberately designing Web-content policies (same principle as newspaper editorial policies) that improve the ability of Soldiers and Army civilians to better perform their missions by keeping them informed of Army policies and programs, and of the individual’s role in accomplishing Army missions.³²⁰

Beyond working with the news media, Public Affairs is an important part of an organization’s Web presence as the proponent for information in the public domain, since as stated, IAW Paragraph 5-2d(3), AR 530-1, when information is not cleared for posting on the WWW, it cannot be released into any other public forum. As the local Web-content manager, PAO should help ensure that corporate content does not release information on one public venue when it is prohibited in another venue. This takes a broad overview more suitable to Public Affairs than to G-6 / DOIM organizations. Adopting a Web-manager approach for all PAOs will also help ensure that strategic-communication themes, both Army-wide and local, are included.

WEB MANAGER VS. WEB-CONTENT MANAGER

As we said in Chapter 1, AR 25-1 uses the terms *Web manager* and *Web maintainer* as synonyms for *Webmaster*, but that’s not what we’re talking about here. PAO’s role in Web content is a sore point with some in the IT world, as “technical control”³²¹ to some means “total control.” Not so. As we explained in Chapter 1, G-6 / DOIM Internet management heavily emphasizes IT – the computers and the networks; i.e., the means of the content’s delivery – as well as the format the content appears in (enabled by what-you-see-is-what-you-get, or WYSIWYG, software) and the policies for managing IT. On the other hand, PAO Web management specifically encompasses content, including the messages behind the content and the command’s relationships with the public.

Perhaps the picture will be clearer if we explain *technical control*. As defined by AR 25-1, *technical control* is “[t]he authority for one organization or command to issue and enforce policy and authoritative direction concerning the use of techniques, procedures, standards, configurations, designs, devices, and systems to another specified organization to accomplish a specific mission. Technical control does not include command authority or administrative control for logistics or matters of administration, discipline, internal organization, or unit training.”

³¹⁵ Paragraph 3g, DoDD 5122.05.

³¹⁶ Paragraphs 3j and 3k, DoDD 5122.5.

³¹⁷ Paragraph 2-3a(4), AR 360-1.

³¹⁸ Paragraph 7a, Enclosure 2, DoDI 5400.13.

³¹⁹ Paragraph 13-1a, AR 360-1.

³²⁰ Paragraph 13-1b, AR 360-1.

³²¹ We’re referring to Paragraph 6-7a(13)(c), AR 25-1: “Webmasters/maintainers will have technical control over the site’s content and will ensure the site conforms to Defense and Army policies, standards, and conventions.”

This definition does not mention management of content anywhere, and it specifies that technical control does not equal command authority – i.e., total control / primary oversight; it focuses on who is responsible for applying the technical skills and techniques required to support the DoD Information Enterprise (DDIE) and to exercise the federally mandated responsibilities for establishing and managing DoD / Army knowledge-management efforts.³²² Therefore the G-6 / DOIMs are charged to consider information a “strategic asset” to DoD and thus secure it; ensure that it is shareable and made available “throughout the information lifecycle to any DoD user or mission partner to the maximum extent allowed by law and DoD policy”; and that any of their IT solutions provide “reliable, timely, accurate information that is protected, secure, and resilient against information warfare, terrorism, criminal activities, natural disasters, and accidents.” In the previous chapter, when we discussed QI, we said that the standard of *integrity* was the responsibility of IT professionals. They are responsible for ensuring that all aspects of the DDIE – including the Global Information Grid (GIG) infrastructure and enterprise services and solutions – are planned, designed, developed, configured, acquired, managed, operated, and protected to achieve a net-centric environment as envisioned in our country’s national-defense strategy.

Therefore IT professionals, called in AR 25-1 as “Website managers / maintainers,” typically have the following technical responsibilities in managing Army Websites:

- Comply with Web-management policy in AR 25-1 and the DoD Web policy, as well as all other DoD guidance and direction.³²³
- Serve as Webmaster / maintainer for each of their Websites / pages, assigned by their organizations.³²⁴
- Register their public Websites with the Army Webmaster at <http://www.army.mil> and update the registration information as changes occur. The registration requirement is specifically designed to assist the American public in locating government information resources.³²⁵
- Serve as a top-level administrator for the primary organizational presence / space on the AKO / DKO portal, as assigned by his / her organization. Coordinate with delegated administrators to manage content within subordinate organizations.³²⁶
- Ensure that management and use of public and non-public Websites is consistent with DoD and Army policy on official and authorized use of telecommunications.³²⁷

“You can have the best infrastructure in the world, but if you don’t have great content, you don’t have a Website.” – Richard Stapleton, senior policy adviser and national Web-content manager for the Health and Human Services Department, quoted in “A Tangled Web We Weaved,” **Government Computer News**, April 2, 2007

³²² DoDD 8000.01, *Management of the Department of Defense Information Enterprise*; Paragraph 1-6c, AR 25-1.

³²³ Paragraph 6-7a(8), AR 25-1.

³²⁴ Paragraph 6-7a(13), AR 25-1.

³²⁵ Paragraph 6-7c(2), AR 25-1.

³²⁶ Paragraph 6-7d(3), AR 25-1.

³²⁷ Paragraph 6-7a(9), AR 25-1. Authorized and prohibited uses of telecommunications are outlined in Paragraphs 6-1e and 6-1f, AR 25-1, and Paragraphs 4-5a(1) and (3) plus 4-5r(7), AR 25-2. Use of telecommunications, including computers, must be IAW legitimate public interest and may not adversely affect performance of official duties by the employee or employee’s organization; may not adversely reflect on DoD or the Army; may not be uses that are incompatible with public service; must be of reasonable duration (normally five minutes or less) and frequency (twice per day), and, whenever possible, are made during the employee’s personal time, such as during lunch, break, and other off-duty periods; are not used for activities related to operating a private business enterprise; may not be for unlawful activities, commercial purposes, or in support of for-profit activities, personal financial gain, personal use inconsistent with DoD policy, personal use that promotes a particular religion or faith, or uses that violate other Army policies or laws – this may include, but is not limited to, violation of intellectual property and copyright laws, gambling, support of terrorist or subversive activities, and sexual or other forms of harassment; may not be political transmissions, including transmissions that advocate the election of particular candidates for public office; and may not cause, directly or indirectly, congestion, delay, or disruption of service to any computing facilities or cause unwarranted or unsolicited interference with others’ use of communications. AR 25-2 specifically prohibits on a government-provided IS or connection 1) “unlawful or unauthorized” activities such as file-sharing of media, data, or other content protected by federal or state law, including copyright or other intellectual-property statutes; and 2) modification of the IS or software, use of it in any manner other than its intended purpose, or adding user-configurable or unauthorized software such as, but not limited to, commercial instant messaging, commercial Internet chat, collaborative environments, or peer-to-peer client applications. AR 25-2 explains that these applications create exploitable vulnerabilities and circumvent normal means of securing and monitoring

- Serve as senior authority for VI, and manage non-tactical VI and multimedia products per OMB Circular A-130, DoDD 5040.2, DoDI 5040.4, DoDD 5040.5, DoDI 5040.6, DoDI 5040.7, and 36 CFR, as defined in Chapter 7, AR 25-1.³²⁸
- Keep records of reviews, IAW DA PAM 25-1-1, Paragraph 7-7j, as well as AR 380-5, Paragraphs 1-13 and 4-15b. Keep written records of violation notifications. Manage Web records per OMB Circular A-130 and guidance from NARA (see 36 CFR 1220-1238 and www.archives.gov/records_management/index.html).³²⁹
- Serve as the appeal authority and liaison with TRADOC G-6 (if at MSO / CoE level) or Army G-6 (if at TRADOC level) to receive and resolve QI appeals.³³⁰

TR 25-1 brings in a further application at MSO / CoE level. IAW TR 25-1, persons managing public Websites fall into two categories: the person responsible for maintaining the organization's public Website, who is known as the *mission Webmaster*, and the person responsible for maintaining the organization's portal, who is known as the *portal administrator*. All TRADOC public sites must have a primary mission Webmaster or portal administrator designated in writing by a commander / supervisor.³³¹ (*Note:* Portals are included in this **Guide** because they are deemed publicly accessible Websites, per TR 25-1. Logically, of course, if the portal is access-controlled with a positive control (see "public accessibility and security" section later in this chapter), it is not a publicly accessible Website and this **Guide** does not apply.)

Mission Webmaster. The mission Webmaster's functions are detailed in Paragraph 5-5, TR 25-1. The mission Webmaster administers and maintains the command / activity's public site, which includes managing the information / content lifecycle in repositories, databases, Websites, and shared drives; ensuring the organization's functional information is current and valid; and ensuring outages are resolved. The mission Webmaster should have a good working relationship with the TRADOC senior commander's and garrison commander's PAO.

Typical responsibilities for the mission Webmaster include:³³²

- Review Web content quarterly to ensure that the posted content complies with DoD Web policy, AR 25-1, DA PAM 25-1-1, and subsequent DoD, Army, and TRADOC directives. Establish local policy as required, in conjunction with the Web-content manager (the TRADOC senior commander's PAO). As part of this function, the mission Webmaster keeps the mission Web-content manager informed about, and ensures quick resolution of, content problems the mission Webmaster identifies.
- Coordinate with the TRADOC senior commander's PAO on the adoption of an effective pre-dissemination content-review process at organization level. Other people the mission Webmaster should work in conjunction with on this project should include the command's portal administrator, OPSEC officer, and other SMEs such as the SJA and security experts.
- Work with the mission Web-content manager to ensure that all content inappropriate for general-public viewing is located in an approved TRADOC knowledge environment. Restricted access by domain or IP address only (i.e., .mil-restricted) is not sufficient for content inappropriate for public viewing; FOUO information, for example, must be contained in a TRADOC restricted-access portal – such as an AKO team site, TRADOC Knowledge Environment (TKE), or Battle Command Knowledge System (BCKS) – or other means of restriction requiring client / user authentication. (See Paragraph 5-3, TR 25-1, and the "public accessibility and security" section later in this chapter.) AKO is the Army's intranet and the preferred site for non-public content.³³³ According to TR 25-1, all organizations listed in TR 10-5 will

network activity, and provide a vector for the introduction of malicious code, remote access, network intrusions, or the exfiltration of protected data. AR 25-2 also states that "[c]ertain activities are never authorized on Army networks. ... These activities include any personal use of government resources involving pornography or obscene material (adult or child); copyright infringement (such as the sharing of copyright material by means of peer-to-peer software); gambling; the transmission of chain letters; unofficial advertising, soliciting, or selling except on authorized bulletin boards established for such use; or the violation of any statute or regulation.

³²⁸ Paragraph 2-1o, AR 25-1.

³²⁹ Paragraph 8-1g, DA PAM 25-1-1.

³³⁰ Paragraph 2-1s, AR 25-1.

³³¹ Paragraph 5-5, TR 25-1.

³³² See Paragraphs 1-5f and 5-5, TR 25-1, for more information on mission Webmaster and portal administrator functions and responsibilities.

³³³ Paragraphs 5-2a and 5-3a, TR 25-1. AKO is authorized for content up to unclassified / FOUO or CUI, according to ALARACT 089/2008, "Securing AKO Content and Credentials (NIPR)," March 25, 2008, but "[w]hen determining access

have a KC on AKO and use it for content that must be available to the Army community. Content not approved for the public domain may be posted to organizations' AKO KC(s).

- Coordinate establishment of new Websites with the TRADOC Webmaster (monr.webmaster@monroe.army.mil), supporting PAO, OPSEC officer, and SJA.
- Chair or co-chair the organization's WWG and organize meetings, conferences, or forums on Internet issues. Serve on the organization's WCWG and OWG.

Portal administrator. AKO-based organizational portal administrators also manage a type of publicly accessible Website³³⁴; portals are also subject to DoD, Army, and TRADOC policies and guidance on Web content. Portal administrator functions are also detailed in TR 25-1. Portal administrators manage the command / activity AKO portal presence, which includes managing the information / content lifecycle in repositories, databases, and shared drives, and ensuring that the organization's functional information, if included in the portal, is current and valid. The portal administrator should also have a good relationship with the TRADOC senior commander's PAO.

Typical responsibilities for the portal administrator include:³³⁵

- Coordinate – in conjunction with the mission Webmaster, TRADOC senior commander's PAO, OPSEC officer, and other SMEs such as the SJA and security experts – adoption of an effective pre-dissemination content-review process at organization level.
- Establish a process for quarterly review of the portal. Quarterly review, at a minimum, should include checks for security risks and design deficiencies, as well as content (post-dissemination) to ensure continued compliance with DoD Website administration policy, AR 25-1, DA PAM 25-1-1, and subsequent DoD, Army, and TRADOC directives. As part of this function, portal administrators should inform the Web-content manager about, and work to ensure quick resolution of, content problems the portal administrator identifies during his / her quarterly review. This may include content on the portal that violates FOIA³³⁶ and should be released to the public domain, for instance.
- Ensures that all content inappropriate for general-public viewing is located in an approved TRADOC knowledge environment. Restricted access by domain or IP address only (i.e., .mil-restricted) is not sufficient for content inappropriate for public viewing; FOUO information, for example, must be contained in a TRADOC restricted-access portal – such as AKO team sites, TKE, and BCKS – or other means of restriction requiring client / user authentication. (See Paragraph 5-3, TR 25-1, and the “public accessibility and security” section later in this chapter.)
- Serve on the organization's WCWG, WWG, and OWG.

Obviously the roles and responsibilities of PAO and G-6 / DOIM (i.e., Web managers, mission Webmasters, or portal administrators) are very different, so it's childish to argue over who has “control.” One has control of the content; the other is challenged with IT and IS issues as mentioned in Chapter 1. As also outlined in Chapter 1, the local PAO and local DOIM should share responsibility for the post's Website, but there's no question that Websites are / should be a primary PAO function. Websites are CI, community-relations, and media-relations venues all rolled into one information tool. PAOs coordinate with other installation entities to accomplish this mission, as required by the interdisciplinary approach, but by charter solely speak for the commander as the “one voice” (command spokesperson).

At the 2008 Army Worldwide Public Affairs Symposium, we heard a PAO remark to another that he had turned over the post Website to his DOIM because he “didn't have time for it.” If you're one of those PAOs who don't claim your post Website as one of your primary functions, why not? Take ownership of one of the most important information tools your command has. Only you can provide the overall perspective and see Public Affairs

controls on AKO NIPR, consider that information which is unclassified or FOUO / CUI may become sensitive or even classified in the aggregate.”

³³⁴ Paragraph 5-5c, TR 25-1.

³³⁵ See Paragraphs 1-5f and 5-5, TR 25-1, for more information on mission Webmaster and portal administrator functions and responsibilities.

³³⁶ IAW Paragraph 8-5g, AR 25-1: “The FOIA program implements the DoD policy that requires its activities to conduct business in an open manner and to provide the public a maximum amount of accurate and timely information concerning its activities, consistent with legitimate public and private interests of the American people.” See Chapter 3 for more information on FOIA.

sensitivities that DOIM personnel will miss. You should be the last stop and last set of eyes before content goes “live” on the public Webserver. And the Web should be a priority – it shouldn’t languish behind other things on

“Many Webpages are developed without regular feedback or testing with customers. When people do provide feedback or ideas, they often never hear what the government will do with their suggestions. Agencies should be required and funded to regularly solicit public opinion and analyze customers’ on-line preferences – just as Amazon, eBay and other top commercial Websites do. This can be done on an ‘opt-in’ basis and without tracking [PII] by using blogs, on-line surveys, a ‘Citizens Insight Panel’ (such as that used by the Canadian government), or similar tools.” – **Putting Citizens First: Transforming On-line Government**, Federal Web Managers Council whitepaper

your plate. People look at Websites and judge the command / commander quicker by the command’s Website than by any other information tool there is. Not to mention that newspapers are dying – all newspapers, including Army newspapers; it’s predicted that soon an Internet presence is all the news and information presence you’ll have. If you abandon control of content to the DOIM now, you will never gain it back unless the guy or gal with stars on his / her shoulders orders it, and even then you will be far behind on what you need to do. You will have lost momentum on communicating to key audiences that you will never overcome.

GENERAL FEDERAL REQUIREMENTS

Part of the necessary responsibilities of a Web-content manager is to ensure that his / her Website meets the general federal requirements laid out in OMB memo M-05-04. As Clay Johnson III, OMB’s deputy director for management, said, a federal Website does not belong to the federal organization to do “whatever” with: “The efficient, effective, and appropriately consistent use of federal-agency public Websites is important to promote a more citizen-centered government. Federal-agency public Websites are information resources funded in whole or in part by the federal government and operated by an agency, contractor, or other organization on behalf of the agency. They present government information or provide services to the public or a specific non-federal user group and support the proper performance of an agency function.”

There are 10 standards for public Websites established at the federal level.³³⁷ These standards – which fulfill the requirements of Section 207(f) of the E-Government Act of 2002 (Public Law 107-347) – are reflected in DoD and Army policy for Websites. Web-content managers must ensure that, overall, management of the ACOM / MSO / CoE public Website is in compliance with federal IRM law and policy. Strategic planning, policy, and best-practices coordination is required with the federal standards, not just black-and-white obedience to Army regulations as expected for compliance to the general military requirements outlined in Chapter 2.

The first federal standard is to establish and maintain information-dissemination product inventories, priorities, and schedules. OMB Circular A-130 and the PRA³³⁸ require federal public Websites to disseminate information to the public in a timely, equitable, efficient, and appropriate manner, and to maintain inventories of information-dissemination products. The E-Government Act requires organizations to develop priorities and schedules for making government information available and accessible to the public, IAW public comment, and to post this information on the organization’s Website. This standard also includes a reporting requirement; an organization must plan and post updates to its final determination of inventories, priorities, and schedules, and to include that information in its E-Gov Act report.

³³⁷ OMB memorandum M-05-04, “Policies for Federal Agency Public Websites,” Dec. 17, 2004.

³³⁸ OMB Circular A-130, Section 8(a)(5), is available at <http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf>. The PRA is available at http://www.archives.gov/federal_register/public_laws/paperwork_reduction_act/3501.html. The PRA provides guidance and requirements for implementation of surveys / questionnaires for which the public may be an audience. All surveys conducted on publicly accessible Websites must include an OMB control number – which is provided following submission and approval of PRA application. It can take up to six months to obtain OMB approval for survey questions. However, open-ended questions don’t require OMB approval. If an office requires a survey to be administered on a public site, such as a user-satisfaction survey, consider contacting the Army Research Institute (ARI), as guidance concerning surveys can be conflicting; per an email from ARI July 22, 2009, Website customer-satisfaction surveys do not require approval. However, surveys and other Army information-collection efforts must also comply with AR 380-13, *Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations*.

The **second federal standard** is to ensure **information quality**. The Information Quality Act, discussed in the previous chapter, requires organizations to maximize their Website content's quality, objectivity, utility, and integrity. This includes making information and services available to the public on a timely and equitable basis. Organizations must reasonably assure suitable information and service quality, consistent with the level of importance of the information. Reasonable steps include: 1) clearly identifying the limitations inherent in the information-dissemination product (for example, the possibility of errors, degree of reliability, and validity) so that users are fully aware of the quality and integrity of the information or service; 2) taking reasonable steps to remove the limitations inherent in the information; and 3) reconsidering delivery of the information or services. (See the QI section in the previous chapter and the definitions section for details on the QI standards of *quality*, *objectivity*, *utility*, and *integrity*. Also see Section 515 of the Information Quality Act, Public Law 106-554; OMB guidelines; and other references.)

The **third federal standard** is to establish and enforce explicit agency-wide **linking policies** describing management controls for linking within and beyond the organization (which the DoD Web policy has done – we'll discuss external links and linking policies later in this chapter). The policies must appropriately limit external linking to information or services necessary for the proper performance of an agency function (in military jargon, "valid mission need"), and must include reasonable management controls to assure that external links remain active or otherwise continue to provide the level of quality (including objectivity, utility, and integrity) intended by the organization and expected by the Website's users.

It should be noted that OMB's information-quality guidelines exclude hyperlinks from its definition of "information" (although links are considered Webpage content), but this exclusion does not remove organization responsibility to exercise due diligence when determining whether to link externally. When an organization determines that external links are necessary for, and material to, the presentation of its information or to delivery of services as part of properly performing one or more of its functions, it must take reasonable steps to ensure that the presentation (and therefore content at the links, by derivative) is accurate, relevant, timely, and complete.

Agencies must reasonably assure suitable information and service quality of external links, consistent with the information's level of importance, and using the same "reasonable steps" listed in the first standard. Although OMB advises caution in this standard on linking to commercial organizations or interest groups due to endorsement considerations,³³⁹ DoD guidance is more restrictive – DoD prohibits linking to commercial organizations or interest groups unless a disclaimer is employed IAW the DoD Web policy.

There are several mandated links, and a mandatory linking policy that identifies those mandatory links and posts (or links to) the following information on an organization's principal Website and major entry points to the site:

- The organization's strategic plan and annual performance plans;
- Descriptions of the organization's structure, mission, and statutory authority;
- Information made available under FOIA;
- Specific Website privacy policies;
- Link to USAGov.gov;
- Summary statistical data about equal-employment-opportunity complaints filed with the agency, and written notification of "whistleblower" rights and protections as required by the No Fear Act of 2002;
- The agency point of contact for small businesses as required by the Small Business Paperwork Relief Act of 2002; and
- Other cross-government portals or links required by law or policy.

The **fourth federal Website standard** is to establish and maintain **communications with members of the public**, and with state and local governments, to ensure that the federal organization creates information-dissemination products meeting their respective needs. To determine those needs, the PRA requires organizations to manage information

³³⁹ Paragraph 3E, Attachment, OMB memorandum M-05-04: "Agency links to commercial organizations or interest groups present special challenges with respect to maintaining agency objectivity and thus must be used judiciously."

collections from the public, or state and local governments (such as Website surveys or questionnaires) as prescribed in OMB's guidance at 5 CFR Section 1320.³⁴⁰ (See Footnote 338, Page 134.)

The **fifth federal standard** is to **assist the public in locating government information** – the principal public Website and major entry points must include a search function. Organizations may determine, in limited circumstances (for example, small Websites), that sitemaps or subject indexes are more effective than a typical search function. The search function should permit searching of all files intended for public use, display search results in order of relevancy to search criteria, and provide response times appropriately equivalent to industry best practices. (The Army's DA PAM 25-1-1 spells out the standards of the search function in more detail.) Websites should provide data in an open, industry-standard format, permitting users to aggregate, disaggregate, or otherwise manipulate and analyze the data to meet their needs.

The **sixth standard** is to use **approved domains**. (See DoDI 8410.1.) Federal agencies may use only .gov, .mil, or fed.us (DoD is limited to .mil) unless the agency head explicitly determines that another domain is necessary to properly perform an agency's function. For the Army, "agency head" is not delegated below CIO / G-6. The standard allows that "proper performance of agency functions" includes an obligation to the organization for clear and unambiguous public notification of the organization's involvement in, or sponsorship of, its information-dissemination products, including public Websites. (The Army's requirement for Webpage titles to contain information on the site's sponsor addresses this.) The federal standard also recognizes that, in certain limited circumstances, other domains may be necessary for the proper performance of an agency function. Approved exceptions to the .mil domain are in DoDI 8410.1.

"All federally owned, managed, and / or directly funded Websites must be hosted on .gov, .mil or fed.us domains." – **Putting Citizens First: Transforming On-line Government**, Federal Web Managers Council whitepaper

The **seventh standard** is for federal organizations to implement **security controls**. DoD's and the Army's more stringent controls are discussed later in this chapter, but the minimum federal standards are in OMB Circular A-130, Appendix III; OMB memorandum M-04-25, "Reporting Instructions for the Federal Information Security Management Act [FISMA] and Updated Guidance on Quarterly IT Security Reporting"; National Institute of Standards and Technology (NIST) Special Publication 800-44, "Guidelines on Securing Public Web Servers"; and other associated guidance from NIST.³⁴¹ Adequate security controls must be in place to ensure that information is resistant to tampering to preserve accuracy; remains confidential as necessary; and the information or service is available as the organization intends and as expected by the Website's users. Agencies must also implement management controls to prevent the inappropriate disclosure of sensitive information; the Army's management controls are discussed later in this chapter.

The **eighth federal standard** is to **protect privacy** and to not disclose information about personnel by implementing OMB Circular A-130's Appendix I and OMB memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002."³⁴² Protecting personnel privacy is a particular concern for the Army.

The **ninth standard** is for public Websites to maintain **accessibility**, discussed in greater detail in the "Section 508" section of this **Guide**, Page 177. Every federal agency must ensure accessibility for individuals with disabilities by implementing Section 508 of the Rehabilitation Act (29 USC 794d). Federal-agency public Websites must be designed to make information and services fully available to individuals with disabilities.³⁴³ Also, organizations are required to provide appropriate access for people with limited English proficiency by implementing DoJ guidance for EO 13166, "Improving Access to Services for People with Limited English Proficiency." Organizations must determine whether an individual document on their public Website requires translation.³⁴⁴

³⁴⁰ See http://www.access.gpo.gov/nara/cfr/waisidx_99/5cfr1320_99.html; Section 8(a)(6), OMB Circular A-130, <http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf>; PRA, http://www.archives.gov/federal_register/public_laws/paperwork_reduction_act/3501.html.

³⁴¹ OMB Circular A-130, <http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html>; M04-25, <http://www.whitehouse.gov/omb/memoranda/fy04/m04-25.pdf>; FISMA, <http://csrc.nist.gov/policies/FISMA-final.pdf>; NIST 800-44, <http://csrc.nist.gov/publications/nistpubs/800-44/sp800-44.pdf>.

³⁴² M-03-22 is available at <http://www.whitehouse.gov/omb/memoranda/m03-22.html>.

³⁴³ More information on Section 508 is available at <http://www.access-board.gov/index.htm>.

³⁴⁴ More information is available at <http://www.usdoj.gov/crt/cor/Pubs/lepqa.htm>.

“Agencies should be funded and required to follow the latest best practices in Web search. This will improve the quality and findability of on-line government information, and help agencies deliver the services most requested by their customers.”
– **Putting Citizens First:**
Transforming On-line Government,
Federal Web Managers Council
whitepaper

The 10th standard, like the first, is a record-keeping requirement. Organizations must meet records-management requirements by implementing OMB Circular A-130 and NARA guidance.³⁴⁵ See provider and reviewer responsibilities in Chapters 2 and 3.

WHEN TO USE AKO; WHEN NOT TO

Web-content managers must also be alert to what their organizations are placing on AKO. Have you thought about it: what *do* you have on your organizational AKO site? Is it there to get around a review process or around a PII requirement? Do the policies still exist that led you to post it to AKO in the first place? And does it meet the FOIA exemptions for being restricted content? (See Chapter 3.)

The Obama administration has said that the federal government will be open and transparent, adopting “a presumption in favor of disclosure.” New FOIA guidelines were issued March 19, 2009, by the U.S. attorney general. We can anticipate a need to evaluate

what we have on AKO for possible move to the publicly accessible Web, and we can expect a more rigorous insistence that information must meet a FOIA exemption to be withheld or restricted via AKO or other means. (You may remember from the Chapter 3 discussion that, by definition, only if information matches one of the specific FOIA exemptions is it FOUO, although it may be “sensitive” or CUI under AR 530-1 and / or AR 380-5.

Posting content to AKO for your convenience – because you didn’t want to follow a policy or procedure – should be a no-go anyway, but we recommend that you evaluate the content you are withholding from the public to see if AKO is truly its proper home. But keep in mind that if content is moved to the publicly accessible Web, the information must be validated for release IAW DoD Web policy et al, and thus the review / clearance procedures outlined in Chapter 3 apply.

Having said this, we’ll discuss when to use AKO. That’s fairly easy to figure out, since AR 25-1 specifies some instances:

- **The installation telephone directory must be on AKO, not on the Internet** – Each Army installation is required to publish an unclassified organizational telephone directory at least annually. Electronic versions of the directory must be placed on the organization’s AKO / DKO community pages (or on AKO-S, as appropriate), but not on the publicly accessible Web. Individual names and office information may be on the directory within the AKO / DKO community page, but organizations must use the AKO / DKO whitepages as their primary tool for individual locator information.³⁴⁶
- **When you need a collaboration and coordination site** – Collaboration and coordination must be done on the non-public (private) side, where the Web manager installs the required access-control mechanisms.³⁴⁷ The AKO portal is considered the primary source for collaboration and coordination.³⁴⁸ In fact, Army commands *must* staff unclassified draft publications and forms electronically by posting them to AKO / DKO or AKO-S, and send email notifications of the document’s presence on AKO / DKO that include the link to AKO / DKO rather than attaching files to the email for review. Further, access to draft documents on a Website must be limited to activities involved in staffing and reviewing the publication or form. Draft publications *will not* be displayed on public-access Websites.³⁴⁹

Organizations are required to use AKO / DKO or AKO-S “to the maximum extent possible to develop knowledge networks and portals inside AKO / DKO.”³⁵⁰ However, there may be times when AKO / DKO resources cannot support an organization’s functional requirements and so the organization is authorized to host a private Website off

³⁴⁵ See 36 CFR, Parts 1220-1238; for more information, http://www.archives.gov/records_management/index.html.

³⁴⁶ Paragraph 6-4r, AR 25-1.

³⁴⁷ Paragraph 6-7a(15), AR 25-1.

³⁴⁸ Paragraph 6-7a(2), AR 25-1.

³⁴⁹ Paragraph 9-2c, AR 25-1.

³⁵⁰ Paragraph 6-7d(1), AR 25-1.

AKO / DKO.³⁵¹ That private Website, however, must be on the .mil domain,³⁵² and it is still considered an official Army Website.³⁵³ An example of a private Website that AKO / DKO cannot support is the unclassified extranet, which is a private Website used for exchanging non-public-domain information with members of the public and other individuals not authorized to use DoD PKI resources.³⁵⁴

A more subjective requirement is that Army public Website content must be “appropriate for the general public,” and if it is not, the content possibly should be on AKO. Even if the content provider and / or organizational Webmaster have done so, Web-content managers must thoroughly evaluate content for its necessity – an assessment of valid mission need, in other words – and consider which venue the content would best fit: the general-public Web, the organization’s portal, on restricted areas within the portal, or on AKO knowledge centers / communities of practice, AKO team sites, TKE, or BCKS, as appropriate. DoD Website policy states: “Only information of value to the general public and which does not require additional protection should be posted to publicly accessible sites on the [WWW]. Information requiring additional protection, such as [FOUO] information, information not specifically cleared and approved for public release, or information of questionable value to the general public and for which worldwide dissemination poses an unacceptable risk to the DoD, including military personnel and civilian employees, should be placed on Websites with security and access controls.”³⁵⁵ Therefore the conditions for content to be placed on the publicly accessible Web are that the content must be of value to the general public, and that the content does not require additional protection. (The content must meet both standards.)

IAW the DoD Web policy, then, information that requires additional protection is:

- FOUO;
- Information not specifically cleared and approved for public release; or
- Information of questionable value to the general public and for which worldwide dissemination poses an unacceptable risk to DoD.

The organization’s general-public Website must comply with Army requirements that “Websites should be made publicly accessible on the Internet only when the target audience includes the public at large. Information that is for Army personnel only should be moved to AKO or placed in a separate, clearly labeled part of your Website.”³⁵⁶ The Army intends that private (intranet) Websites reside on AKO; see Paragraphs 6-7d and 6-7e, AR 25-1.

Therefore, in addition to the examples specified by AR 25-1, the proper use of AKO is for FOUO information, uncleared content, or information meant exclusively for organization employees and of little or no use to the private sector – according to Army policy, if information is for an organization’s exclusive use, it must be contained in AKO “or other approved intranet (private) site.”³⁵⁷ (Note: “Uncleared content” is a temporary state, meant for draft content, and is not to be used to avoid the content-review process, which is outlined in Chapter 3.) Inversely, content on an Army public site – which includes the organization’s non-access-controlled portal – must include only information of value to visitors ranging from private industry to citizens with an interest in the missions performed to users from Army organizations, other government agencies, and academies.³⁵⁸

Content on the HQ TRADOC, MSO, or CoE homepages pointed exclusively toward organizational employees may be considered in emergency or other exceptional situations; the organization’s contingency and continuity-of-operations plan (COOP) should outline this provision. (See Page 140.)

Again, the security approach is evident throughout this requirement, but on the other hand, remember that the “public at large” actually “owns” the public Website, and therefore content on it must cater to them. This does not mean that security can be ignored. As AR 25-2 states, use of government IS and access to government networks is a “revocable privilege, not a right.”³⁵⁹ All IS users are charged to mark and safeguard files per their classification level and to disseminate them only to people authorized to receive them with a valid need to know,³⁶⁰ which

³⁵¹ Paragraph 6-7e(1), AR 25-1.

³⁵² Paragraph 6-7b, AR 25-1.

³⁵³ Paragraph 6-7a, AR 25-1.

³⁵⁴ Paragraph 6-7e(6), AR 25-1.

³⁵⁵ Paragraph 3.3, Part II, DoD Web policy. See also Paragraph 3.6.1.

³⁵⁶ Paragraph 8-1a, DA PAM 25-1-1.

³⁵⁷ Paragraph 8-2e, DA PAM 25-1-1.

³⁵⁸ Paragraph 8-2a, DA PAM 25-1-1.

³⁵⁹ Paragraph 3-3c, AR 25-2.

³⁶⁰ Paragraph 3-3c(3), AR 25-2.

precludes a “release everything” attitude toward the Internet. Government IS users are further required to practice safe network and Internet operating principles and to take no action that threatens the integrity of the system or network.³⁶¹

There are also “when not to use AKO” considerations and, as may be expected, they also are subjective. These considerations invoke reference to the FOIA discussion of Chapter 3, and they help the organization meet the fifth federal standard mentioned earlier in this chapter. From a Web-content manager’s viewpoint, content on AKO must not violate the FOIA by being information that is mandated for release. In fact, an organization’s public Website and the FOIA integrate when the Website is FOIA-friendly enough that it contains records releasable under the FOIA, precluding the public from being forced to request the information – DoJ’s FOIA Web section, <http://www.usdoj.gov/oip/index.html>, is a good example of a FOIA-friendly Website. DoJ’s FOIA Website contains an “about the organization” section as well as a press room for news releases, a publications and documents portal, and FOIA reading rooms – all which contain information already available to the public. DoJ’s FOIA Website also contains a reference guide, cited in the last chapter, and a list of principal FOIA contacts.

In planning inclusion of a FOIA section on your organization’s public Website, work with your organization’s FOIA officer. Each organization’s FOIA officer is responsible for reviewing the organization’s policies and practices on the availability of public information through Websites and other means, including the use of Websites to make available the records described in Section 552(a)(2) of Title 5, USC.³⁶² Each organization should implement features on its Website that will make processing FOIA requests more streamlined and effective, as well as increasing the public’s reliance on using the Website to retrieve the records that can be made available to them without requiring them to request records under the FOIA.³⁶³ As organizations must provide not just FOIA requesters, but the public in general, citizen-centered ways to learn about the FOIA process, about agency records that are publicly available (make the records available but also provide information in a “reading room” introduction, for instance, about what types of information are publicly available), and about the status of a person’s FOIA request and the agency’s response,³⁶⁴ the public Website is a natural tool in the FOIA and transparency process.

Public Affairs personnel work behind the scenes with the FOIA officer as well as on the organization’s FOIA-specific public-Website content. In a Sept. 17, 2008, memo, the Army Staff’s director and the SecArmy’s administrative assistant charged core members of the FOIA team – FOIA officers, PAOs, SJAs, and initial denial authorities – to coordinate proposed FOIA releases and other releases of information with each other “[b]ecause many Army FOIA releases generate significant public interest and garner national media coverage.” The memo, which was written to commanders, supervisors, and leaders to ensure that the Army responds to FOIA requests in a “consistent, coordinated, and timely fashion,” stressed a needed commitment across the Army to “making timely and accurate responses to requests for information submitted by the public, representatives of the news media, or members of Congress.” Again, the organization’s public Website can be used to buttress that commitment.

The FOIA effort must be coordinated because Army records – via the Web or other venue – may only be released after the FOIA / Privacy Act authority approves their release IAW AR 25-55 and AR 340-21. FOIA / Privacy Act officials who release Army records must inform their PAOs if the records contain controversial information; if denying a request for release of the records will probably be contested; or if the records will be released to a media representative. PAOs, in turn, must notify their commanders and OCPA.³⁶⁵

DoD and Army policy establish required FOIA content for publicly accessible sites, including processes to submit FOIA requests. These requirements will be delineated for the Website coordinator / Web-content manager in this chapter’s “required content” section. At this time, the TRADOC homepage includes a FOIA page linked from the “resource center” page, while a link is provided to the Army’s FOIA page from the footer of www.tradoc.army.mil, to fulfill the requirements.

³⁶¹ Paragraph 3-3c(5), AR 25-2.

³⁶² Section 3(a)(iv), EO 13392.

³⁶³ Section 3(b)(ii), EO 13392.

³⁶⁴ Section 1(b), EO 13392.

³⁶⁵ Paragraph 5-5a, AR 360-1.

“STRATEGIC WEBBING”

Where a Web-content manager’s guiding hand is needed most is in the strategic vision behind the Website. As PAOs, we understand the concepts of “branding” and “speaking with one voice” – those concepts, however, are the tip of the iceberg in portraying a strategy. Army Websites, too, as tools of public and command information, must display these concepts. The links you choose to make and the Webpages you post not only enhance visitor usability but also enhance (or detract from) the Army’s corporate ethos.

On the surface, PAOs help educate their commands about the strategy behind the policy’s requirements so that content providers buy into the strategy rather than feeling “burdened” with requirements. However, “strategic Webbing,” or strategically constructing your organizational Website, is a far deeper strategy, as we’ll discuss following. First, we’ll cover the Army’s minimal requirements vis a vis a strategic vision.

Website purpose (mission) statement and plan. Each Website must have a clearly defined purpose statement and Website plan that supports the organization’s mission.³⁶⁶ The purpose / mission statement should encompass the organization’s key processes.³⁶⁷ The Website plan should be approved by the organization’s parent command or organization, and it must address, at minimum:

- Its Website registration.
- Mission Webmaster / portal administrator contact information. (At a minimum, this must include the mission Webmaster’s / portal administrator’s email address for users to request information or direct questions, comments, suggestions, etc., for that organization.)³⁶⁸
- Procedures that explain posting of information and review of the site for content and format.
- Contingency and continuity of operations, describing what the organization will do with its Website during disasters or emergencies, and what important information and services will be provided to the public.

This Website plan is to be documented along in the organization’s COOP,³⁶⁹ which must comply with Paragraph 6-1b, AR 25-1. TRADOC’s COOP must be modeled after AR 500-3, which requires a plan for re-establishing minimum essential operational capabilities (MEOC) at the facilities TRADOC will relocate to in an emergency. A COOP plans for emergency response, backup operations, transfer of operations, and post-disaster recover procedures each activity maintains as part of its IA security program.³⁷⁰ Each organization must determine how high-level a MEOC its public Website

is – or even if it is considered a MEOC at all; whatever the decision, the organization tells the public what services, including the Website, will be restored, when they are expected to be restored, and what the priorities for restoration are. The Website purpose statement and plan must be robust enough that they can fulfill the conditions implicit in the non-endorsement disclaimers for hyperlinks: “Such links are provided consistent with the stated purpose of this Website.”

The Interagency Committee on Government Information recommends that each organization’s COOP plans cover:

- Situations in which Websites may need to be taken off-line;
- Procedures for bringing Websites back on-line and ensuring access to systems;
- Procedures for updating, approving, and maintaining content in an emergency;

“A long-term plan outlines what you plan to do in the future, but a strategic plan tells you what you’re going to do today to make sure you’re still around in the future.” – *The Handbook of Strategic Public Relations & Integrated Communications*, Clarke L. Caywood, editor

“Each Website shall have a clearly defined purpose that supports the mission of the DoD [c]omponent.” – DoD Web policy, Part II, Paragraph 2.1

³⁶⁶ Paragraph 2.1, Part II, DoD Web policy; Paragraph 8-1c, DA PAM 25-1-1. Expected to also be included in the new AR 360-1 as Paragraph 13-14c.

³⁶⁷ Paragraph 3-2a(1), AR 5-1.

³⁶⁸ Paragraph 5-5b(3), TR 25-1.

³⁶⁹ Paragraph 8-1c(4)(a), DA PAM 25-1-1.

³⁷⁰ Paragraph 4-5i, AR 25-2.

- Procedures for providing critical information that the public expects and needs most; and
- Procedures for collaborating with other agencies to minimize redundancy and to ensure that similar information is consistent and accurate across agencies.³⁷¹

Organizations must consult SMEs as to the markings on their Website purpose statements and plans, as they may require FOUO marking.

See Appendix L, this *Guide*, for a “template” to adapt.

Army policy requires organizations to institute a Website plan but doesn’t give details on the *how* or *why*, although the principles in AR 5-1 for organizations can certainly apply to organizations’ public Websites. This section discusses strategically planning and managing an organizational Website.

Our assessment of TRADOC’s organizational Websites is that they are, by and large, reactive. They respond to the demands of policy or their leaders’ whims, but few are actually backed by *strategic planning*.³⁷² To have a truly robust Web presence, TRADOC should adopt a proactive, customer-service-based, strategic-communication way of thinking about its Web content. This aligns with the concepts outlined for Total Army Quality (TAQ) management in AR 5-1.

We’re not talking about *strategic communication* as the Army practices it via themes and messages. What we mean by strategic communication is **putting our audience first**. To do this, we must adopt strategic Webbing as an ACOM and across all the ACOM’s elements, as strategic Webbing requires a concerted effort among all ACOM organizations.

As illustrated by the quote from *The Handbook of Strategic Public Relations & Integrated Communications* on the preceding page, there’s a difference between a plan for the future and a strategic plan. The strategic plan applies to how you want your Website to grow and develop as well.

Strategically constructing your organizational Website is expected by DoD policy, too, as shown by the excerpt from the DoD Web policy on the preceding page. Implicit in achieving this portion of the policy is a plan: a plan and purpose for the Website that supports the organization’s mission. Out of the mission statement are built the organization’s strategic objectives. If the organization clearly communicates and adheres to its strategic objectives, the content of your organization’s Website will serve its users, or “customers,” better. Not to mention that a badly presented Website with poorly thought-out content will actually do your organization more harm than good since people will judge your organization based on the quality of your Website. If your Website looks bad or has no content “meat” to it, your organization’s and TRADOC’s corporate ethos will suffer.

Thus the need for strategic Website planning. Let’s look at these principles and the steps for achieving them.

- Distill the organization’s essential nature, its values, and its work into a motivating mission statement.
- Building on the organizational mission statement, clarify the purpose of your organization’s Web presence.
- Understand your Website’s customers’ needs via careful analysis.
- Set objectives to communicate what your organization does that will serve those needs. These are your organization’s strategic Website plan goals.
- Target your content, or message, to your customers.
- Evaluate your effectiveness. Keep content fresh.

Step 1, distill the organization’s essential nature, its values, and its work into a motivating mission statement.

A motivating mission statement will be the foundation of your content. But it’s not a mission statement like you’ll find on TRADOC Websites. There are certain things you’re trying to achieve when you write, or rewrite, the mission statement for your organization:

³⁷¹ From http://www.usa.gov/webcontent/governance/policies/emergency_planning.shtml.

³⁷² To adapt Paragraph 3-2a, AR 5-1, to Website strategic planning, *strategic planning* is the process by which high-level managers (Web-content managers and organizational heads) envision their organization Website’s future / goals and develop the necessary procedures and operations to achieve their vision. Website strategic planning is a continuous and systematic effort to determine and meet Website customers’ needs, present and future. Website strategic planning focuses and aligns the organization’s efforts to portray on its public Website the core competencies, key strategies, and actions that must be taken to achieve success for both the organization and its Website.

- The mission/vision statement should act as the organization's guiding light, pointing the way toward the future.
- The organization's purpose should be expressed in an emotional way to inspire passionate support and ongoing commitment.

"The more you know about the environment in which your organization is working, the more effective you'll be in communicating your message." – Janel Radtke, *Strategic Communications for Nonprofit Organizations*

Content must be relevant to the audience: "A long-term relationship with its consumers should be the organization's most important goal. Organizations that embrace consumers as true stakeholders in their success will benefit." (Caywood)

Communication should build trust: "A key component of trust is consistency in behavior and messages." (Caywood)

The public's level of involvement will be determined by the extent to which the audience connects to the situation or issue. Topics of relevance have significant personal consequence.

The outcome of communication "must be defined in terms of desired [audience] behavior." (Caywood)

- The mission statement should include a vision of the future that is possible, articulated in a way that is easy to understand, and 100 percent convincing.
- The mission statement should articulate the organization's values in such a way as to be the motivating force behind everyone connected to the organization.
- The mission statement should use proactive verbs to describe what you do.
- The mission statement should be jargon-free and expressed in language that could be easily understood by an eighth-grader.
- The mission statement should be short enough so that anyone connected to the organization can readily repeat it when asked by anyone else anywhere at any time. We recommend that the mission statement be no longer than five sentences.

A good mission statement should accurately explain why your organization exists and what it hopes to achieve in the future. The organization's mission statement should be motivational. Does your organization's mission statement do these things, or is it rather ho-hum?

To help you craft a mission statement that achieves these things, answer these questions:

- What are the opportunities or needs that our Web presence exists to address? (The *purpose* of the organization's Web presence.)
- What are we doing to address these needs? (The *business* of the organization's Web presence.)
- What principles or beliefs guide our work? (The *value* of the organization's Web presence.)

Step 2, building on the organizational mission statement, clarify the purpose of your organization's Web presence. A number of organizations think they have to have a Web presence but have put no thought into what they expect their Website to do or what they want it to achieve in the future. So we recommend that when you write a mission statement for your organization's Website, you ensure that it supports the strategic goals of your organization and advances its purposes. Explain your organization's Web presence accurately. You should answer the questions in the preceding three bullets while writing a mission statement for your organization,

since the mission of your organization and the mission of your organization's Website are inseparable.

Step 3, understand your Website's customers' needs via careful analysis. An important part in knowing what you want your organizational Website to do is knowing who in cyberspace you want the site to reach. So analyze and focus on who or what your organization exists to serve. Embrace that the Website is a core business function and that you have customers and stakeholders. Think about who your customers or stakeholders are. (We'll come back to customers and stakeholders). Do the annual survey that the Army requires – it could be enlightening. (See Appendix O.)

Step 4, set objectives to communicate what your organization does that will serve those needs; these are your organization's strategic Website plan goals. Now that you have an idea who you are or can be reaching with your Website, you set your objectives for what, how, and why you're communicating; the next logical step – once you've defined your organizational mission, your Website's mission, and your customers – is to then determine what your organization wants its customers to derive from your site. Before you set communication objectives, ask yourself these questions:

- Does your organization's Website help the organization achieve its objectives?
- Why do you have a Website? What's it supposed to accomplish?
- Does your content support that objective?
- What makes your Website different from all the others out there?

Then, as you set your objectives, work within these parameters:

- Goals – focus on **what** your organization wants to make happen. Tips for goal setting:
 - Goals should grow out of your mission.
 - They should have a long-term, big-picture focus.
 - When put together, they comprise an organizational “wish list.”
 - A goal is the end result your organization wants to achieve; every goal should specify what your organization wants to happen and who will be affected by it.
- Objectives – focus on **how** your organization proposes to make its goals happen. Tips for establishing measurable objectives:
 - Set a realistic target date for completion of goal(s).
 - Specify the degree of change – give number of people or percentages of an existing figure, such as percentage of targeted audience, that can be counted and / or measured along the way. What must happen to indicate that something has been accomplished within the targeted audience?
 - If money is used as a measurement, give amount, whether in dollars or percentage of current benchmark. State exactly what you hope to accomplish with those people or that money.
 - Identify the population within which you want to create change.
 - Be specific about what it is you want to accomplish. Five areas need to be clearly defined: area of change, direction of change (i.e., *more* or *less*, and percentage), target audience, degree of change, and timeframe or target date.
- Communication (Website) objective – focuses on **who** needs to be reached and **why**. (Covered more in the “customer” section.)

Principles of relevance:
“Influencing, persuading and motivating this critical stakeholder group [the consumer] is a fundamental activity of any organization. ... Communications are more effective if constructed from the beginning with the wants, needs and motivations of that audience in mind.” (Caywood)

“The relationship between an organization and its consumers is an interdependent one, and one which should work to the benefit of both parties.” (Caywood)

“Communications is about building understanding. It is about nurturing change.” (Radtke)

Step 5, target your content, or message, to your customers. In Step 5, you write the content that is most relevant to your customers. We will come back to messaging, but see the box on the previous page: it has some key principles for messaging.

You may be thinking, “Aw, I don’t need to know this.” However, TRADOC as a whole must commit all our energies to thinking what information products our audience needs and producing those. All information in the public domain is the responsibility of Public Affairs, true, but if this philosophy is adopted command-wide, by all Web content providers, think how powerful this would be.

Step 6, evaluate your effectiveness and keep content fresh. See Appendix O for best practices on how organizations can evaluate their effectiveness. One way to be effective is to change your content frequently. Adding new content gives your Website visitors a reason to return – if they know they’ll see a new thought-provoking article, a new product, a “what’s new” section, a calendar of events relevant to them, or a feature on things to come, they’ll come back to your Website.

How TRADOC can have products, customers. We cannot just “throw” information out there and pretend that it will be of use to someone – that someone will read it. We will miss the mark with that type of thinking. Our “general public” audience on the public-domain Web consists of stratifications. (See Chart 4-1, below.) We have to know the purpose of our communication – and it is not to solely provide information. Optimally, we want our reader to feel, think, or do in response to our information, and therefore the information must be the right message to the right person at the right time – in other words, relevant.

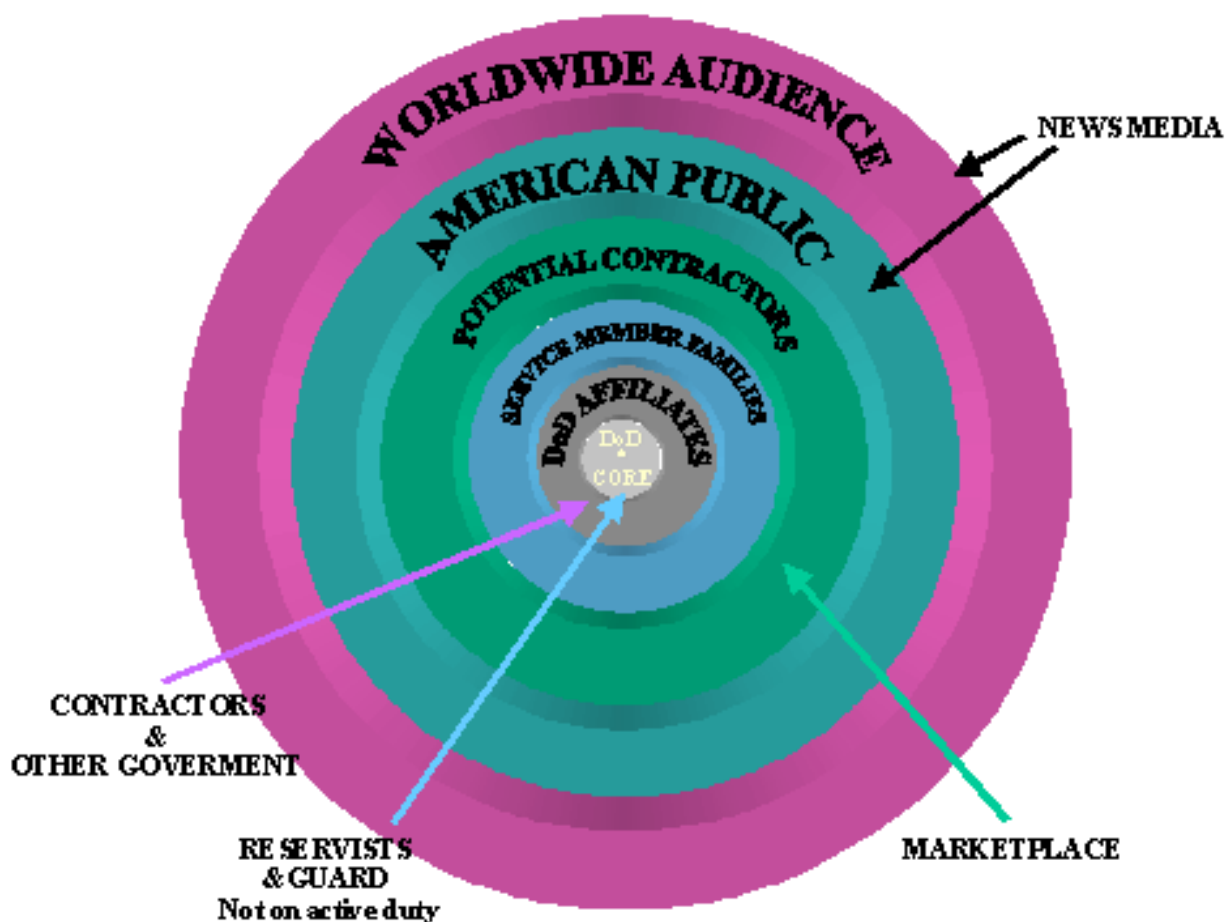


Chart 4-1. The DoD Web policy provides an illustration of DoD target audiences that shows the stratifications of audiences for public-domain Websites. For our purposes here, we will use the terms audience, public, consumer, customer, and stakeholder interchangeably. It is also important to note that, although audiences are shown stratified for thinking / planning purposes, in reality Internet communication reaches across all audiences and cannot be stratified for just one audience.

It used to be that, as defined by communications science, a message was information sent from a source to a receiver, with varying degrees of relevance to the receiver. **Today's world, however, is receiver-centric.** The receiver holds all the cards in how he / she receives messages, and this has major implications for would-be message sources. In fact, a communicator's approach cannot be through methods tried just five years ago, as social media is causing a paradigm shift in how people receive messages and read / share news, information, and other content. Today's consumer of content expects to dialogue with an information source (no more “And that's the way it is” in

the flavor of Walter Cronkite) and to edit (e.g., turn off, snip, repurpose, retransmit, retweet) an information source. Never has it been truer that the medium is the message (Marshall McLuhan).³⁷³

To achieve relevance in this receiver-centric Brave New World, it may help to adopt a business model and think in terms of *products* and *consumers* or *customers*. It may be a transition in mindset to truly think of our Website audiences as our customers or consumers, but since a “consumer is anyone from whom the organization wants something” (Caywood) – and, at minimum, we want people to read our Web content – the customer / consumer, in a sense, is the person who “consumes” our organization’s product or service. IAW TAQ tenets: “All organizations have customers. The sole reason for an organization to exist is to meet or exceed customer requirements. All processes and activities are focused on meeting the current and future requirements of customers. The customer determines the value of your organization based on the quality of the products or services you provide.”³⁷⁴

First, let’s look more closely at what our *product* is, to use a common business term. Our product is tied to the Army’s mission, which is to “provide national defense and security for American citizens – our ultimate customers.”³⁷⁵ Using the TRADOC CG’s vision items on <http://www.tradoc.army.mil/about.htm>, let’s consider the topics, as shown in the Webpage’s bullets, as clues to TRADOC’s product lines, if you will. Each bullet is also a strategic objective. Therefore one of TRADOC’s major products is what we produce to recruit and train Soldiers. Another major product is what we produce to develop adaptive leaders. A third is what we produce to design the modular force and future combat force. A fourth is what we produce to achieve institutional learning and adaptation.

So what do we want from our Website visitors, and what do they need from us? That’s the question each organization must answer for itself, backed by strategic planning and distilled into concrete strategic and action plans. (See AR 5-1; also see Appendix O in this *Guide*.) The consumer for TRADOC is the end-user of our services, the one who benefits from the services our organization has to offer and – an important part of the picture – the one who creates for our organization a sense of purpose and focus. We should not be merely imparting information to our customers, deciding what we think they need vis a vis Web content, but we should be interacting with them, and this gives us purpose and focus. (It is also what they expect in this day-and-age of social media.) If we adapt to this spirit: “[Consumers] are our constituents and we are their representatives,” this gives us far more of a stake in meeting their needs.

In addition to thinking of people as our *customers* or *consumers*, we also must think of them as our *stakeholders*. Simply defined, *stakeholders* include “individuals and organizations that have a ‘stake’ in the failure or success of another organization (Caywood).” Illustrated in the following list are stakeholders for HQ TRADOC; your organization will have many of the same stakeholders:

- Employees, prospective employees, retired employees;
- Global, national, local and trade media;
- Institutional and individual investors – in the Army’s case, the institutional investor is Congress (budget), and the individual investor is the American taxpayer;
- Local, state and regional government – elected and appointed officials, public-interest groups, political party leaders, PACs;
- Leaders and employees in executive, legislative or judicial branches of the federal government; government agencies;
- Professional associations such as the Association of the United States Army (AUSA), Army Aviation Association of America (AAAA); rank associations such as the Warrant Officer Association;
- Educational institutions – college for ROTC base and high schools for the Junior ROTC base;
- Industry partners for TRADOC;
- Community members and leaders;
- Neighbors to Fort Monroe (Phoebus, Hampton);
- American public as supplier of employees (“influentials”);

³⁷³ See http://individual.utoronto.ca/markfederman/article_mediumisthemessage.htm for a thoughtful essay by Mark Federman.

³⁷⁴ Paragraph 3-1d, AR 5-1.

³⁷⁵ Ibid.

- Environmental interest groups for impact of training on environment;
- Unions and related labor interest groups;
- “Big A” Army; and
- “Sister” services.

TRADOC’s biggest consumer / stakeholder probably is the operational Army.

Rule-of-thumb: **any piece of content on the public-domain Web should have at least three stakeholder audiences** – this should help in determining what should be on AKO and what should be in the public domain.

Critical in building a strategically based Website is researching and analyzing your audience, as we’ve been discussing, then determining your audience’s level of involvement. There are several key points about audiences:

- The more specific you can be when defining your key audiences and potential outreach partners, the easier it will be to find the most effective ways to communicate with them.³⁷⁶
- Learn all you can about your audience so that you can “stand in their shoes” and relate to their point of view.³⁷⁷
- Three types of information are usually used to segment audiences: demographic, geographic, and psychographic.
 - Demographics – sex, age, income, education, marital status, occupation, race, family-dwelling location (city, suburb, rural), family size, lifecycle. For the Army audience, occupation and family dwelling location is known, but the variety of family-member occupations, for instance, must be researched.
 - Geographics / geodemographics – this segmentation is done by looking for the average demographic characteristics of a particular geographic area and applying them to everyone in that area. Geographical categories: country (different culture, government, economy), region (different sensibilities, economies), state (different climate, regulations economy), city (pace, culture, politics), zip code (different congressional districts), neighborhood (different stores, parks, restaurants, families, friends), rural (associated with isolation, quiet, hard labor such as farming), town (each has its own unique center), suburb (“culture” of tract housing, strip malls, and giant stores). While IMCOM may find this segmentation to be of value in applying it to audiences surrounding particular installations, a spread-out ACOM may find this category of segmentation to be far less beneficial.
 - Psychographics – use of psychological, sociological, and anthropological factors, such as benefits desired, self-concept, and lifestyle, to determine how the market is segmented by the propensity of groups within the market – and their reasons – to make a particular decision about a product, person, or ideology, or why they otherwise hold an attitude or use a medium. There are three basic categories within this segment: activities (how people spend their time), interests (what’s important to them in their immediate surroundings), and opinions (how they view themselves and the world around them).

In addition to using measurement and survey tools (see Appendix O), to learn all you can about your audiences, you conduct an analysis of your external environmental scan. This scan has three components: public environment, competitive analysis, and macroenvironment.

The *public-environment scan* analyzes which groups of people or which organizations have an interest in the activities of your organization: whether that interest is for or against doesn’t matter. They have a stake in what it is you do and they have an impact – or the ability to impact – your organization.

The *competitive analysis* is a list of groups that compete for the attention and loyalty of the segments of the public you’ve identified as your targeted audiences. These organizations often are viewed as competitors. The competitor organizations may provide similar services to similar audiences, or they may be *perceived* as doing the same things your organization does – whether that is true or not.

The *macroenvironment scan* analyzes the outside forces that shape opportunities and pose threats to the organization – part of the traditional analysis of the organization’s strengths, weaknesses, opportunities, and threats (SWOT).³⁷⁸ By researching five primary areas (demographics, economic, technological, political, and social), your organization

³⁷⁶ Page 41, Radtke.

³⁷⁷ Ibid.

³⁷⁸ Paragraph 3-2d(4), AR 5-1.

can prepare itself to take advantage of opportunities these forces present as well as have ready contingency plans to avoid or lessen the impact of any threat set off by one or several of these five factors.

- Demographics – a shift in the population you serve. (See above.)
- Economic – the perception of the economy will have an impact. Economic indicators may also suggest the need for higher levels of existing services; new service opportunities; or a constituency in the making for a specific policy proposal.
- Technological – advances in technology can create ways of relating to different audiences. Social media is a prime example of this.
- Political – political decisions, especially regarding base realignment and closure (BRAC), will impact the Army.
- Social – changes in the social agenda or cultural norms can affect an organization, either positively or negatively.

“If you want to get your messages across, you need to be a source of information.” (Caywood)

“An organization’s actions have consequences for other organizations or groups of people. It is through this consequential relationship that organizations create publics. Publics are formed when people face a problem, recognize that the problem exists, and organize to do something about that problem.” (Radtke)

“Influencing, persuading and motivating this critical stakeholder group [the consumer] is a fundamental activity of any organization. ... Communications are more effective if constructed from the beginning with the wants, needs and motivations of that audience in mind.” (Caywood)

“While the organization’s goals and objectives are the foundation of its [communications], the message is the heart of its efforts to reach its target audiences. ... Many of us confuse messages with soundbites, taglines, slogans or statements about our organization. While a message may reflect these things – or occasionally incorporate them – it is something much more fundamental and substantive. Indeed, the message is what inspires and anchors soundbites, slogans and taglines.” (Radtke)

The best way to keep abreast of these five areas is to stay informed not only about current affairs but also to conduct informal surveys every six months or so – at least yearly, as the Army requires. Such surveys can help to either confirm or challenge our general perceptions as to where these five forces are heading and what impact to expect and/or plan for.

As a recap to this section, if you accurately define your organization’s “products,” you can better document how those “products” will help your “customers” solve their problems or enhance their lives. In essence, addressing your customer’s needs is one of your Website’s purposes. Posting articles, fact sheets, and whitepapers helps visitors understand what you are trying to accomplish.

True, TRADOC is not in the business of selling a product, but you still “sell” your corporate ethos on the Internet. So use your Website to “sell” your organization. Use email links, fill-in forms, a contact page, a frequently-asked-questions (FAQ) page, “invite ‘em in” links, even a bulletin board or discussion page. If you produce a newsletter or whitepapers, use a subscription form.

Messaging. Our content fails because we don’t have a relevant message. Remember, we are not discussing messaging as the Army practices it, where an Army organization puts forth a statement (usually heavily jargonized) that it wants to deliver, but relevant messaging that the audiences *need* to know. Messages are not just pieces of information; they have inherent calls to action.

What makes a good message? The text should:

- Clearly define the issue or problem;
- Delineate the cause of the issue / problem;
- Connect the issue / problem to the target audience (makes it relevant);
- Indicate a course of action or solution;
- Help the organization achieve its objective;
- Be only one or two sentences; and
- Communicate a complete thought.

“A strong message will define the problem or issue in a specific way, delineating the cause of a problem, which in turn will dictate

the solution,” according to Radtke. The message may define the problem by centering on an individual’s role in the problem and the solution.

Let’s break down a message on the “about TRADOC” Webpage that states how TRADOC develops adaptive leaders: “TRADOC trains leaders for certainty and educates them for uncertainty. Leader development produces innovative, flexible, culturally astute professionals expert in the art and science of the profession of arms and able to quickly adapt to the wide-ranging conditions of full-spectrum operations.”

What is the issue or problem? What is its cause? Most importantly, what is the relevance of the problem to the American public? What do we want them to do about it? How does what we want them to do about it help TRADOC achieve its objective(s)? And all this in just one or two complete sentences!

Message “construction” is not for amateurs or the faint-of-heart, as these small pieces of information are responsible for TRADOC’s success and image in the public’s mind. There are six key steps to developing effective messages:

- Develop key themes;
- Decide on the message “frame”;
- Create an umbrella, or universal, message;
- Use the *message triangle* to develop messages;
- Examine language and symbols; and
- Teach the message to all staff personnel, then let go of it.

Step 1, develop key themes. “Ideally, your organization should have three or four key themes that help you formulate messages that anyone from within your organization can use to talk about the issue with others. These themes provide the emotional grist that best responds to challenges, arguments, or questions that may arise while resonating most readily with a number of populations.” (Radtke) If you recall the previous discussion about TRADOC having “product lines,” you can build key themes around the product lines.

Step 2, decide on the message “frame.” “How you delineate the problem and the cause of that problem will dictate not only the solution and who’s responsible for the solution, but how the entire issue is discussed – or *framed*.” (Radtke)

Step 3, create an umbrella message. “(The umbrella message) is the universal message – the one that defines the organization and clarifies its mission. It has three components. *What it is* defines the organization; *what it means* is why the organization and / or its mission is important to society or the community; *what to do* is what your organization would like to see society or the community do to support the mission. This message encompasses the values and the positions of the organization, which is why it is called an umbrella message. Inasmuch as possible, symbolic language should be used in an umbrella message to capture the attention of both emotional and more rational audience members.” (Radtke) Applied to your organization, its umbrella message should define your command’s core functions and responsibilities (*what it is*) but should also portray its relevance to its higher command, the Army, and the nation (*what it means*). The message also should include what your organization wants from its higher command, the Army, and nation (*what to do*).

The principles behind the umbrella message are:

- “Usually [the ‘what it is’ element] remains constant throughout and is influenced primarily by your organization’s values, knowledge, and experience. It is the common thread that runs through all your messages ..., no matter which audience your organization is addressing. It is this aspect of the message that most effectively frames an issue – e.g., the problem and its cause.
- “Usually it is [the ‘what it means’ element] of the message that gives us the effective lead when addressing a specific target audience because it goes to the heart of audience members’ concerns. Ideally, you want to be able to tailor this in response to different target audiences. Why should an individual pay attention, be concerned, take action? [T]his aspect of the message also can be used to segment audiences.
- “[The ‘what to do’ element] is often the same for several audience groups. ... Obviously, the effectiveness of this type of message may be more difficult to measure. ... This element of the message equation may change over time as the political, social or economic landscape changes.” (all three bullets, Radtke)

The universal message serves as an overall communications goal or objective. As discussed above, it defines the organization and clarifies its mission. To support TRADOC strategic communications, once you have a universal

message, you craft messages that support TRADOC's strategic objectives, keeping in mind that most successful messages are expressed in ways that *resonate* with the perspective, experience, and values of your target audience.

TRADOC's umbrella message is inherent in our slogan, "Victory Starts Here!" ("Victory Starts Here!" is a slogan, not a proper umbrella message.) However, your Website content should portray what part your organization has in ensuring victory.

Step 4, use the message triangle to develop messages. To assist in creating an umbrella message and any "product line" messages, consider building messages on the *message triangle*, illustrated below. The message triangle builds in relevance to the audience and asks for their interaction or to do something.

We acknowledge that building messages on the message triangle is a departure from the way HQ TRADOC STRATCOMMers build messages now, but the message-triangle concept is more likely to keep your messages from being empty slogans. An organization should have three or four key themes based on its strategic objectives. In looking back at the "product lines" from the CG's vision statement, TRADOC has four key themes, but the messages that are part of those themes are too long and not memorable. Even the shorter ones are rather "so-what" messages. They're not relevant to our customers – they don't resonate.

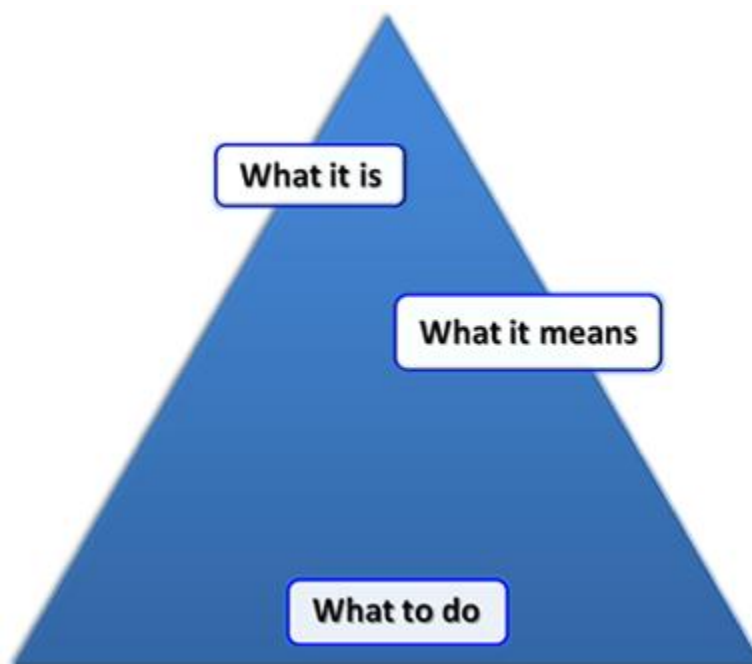


Chart 4-2. The message triangle illustrates the three components of the umbrella, or universal message: what it is, what it means, and what to do. Each component must be answered in constructing a good message. What it is is an explanation of the problem, program, issue, or service. What it means will tell an audience why this issue, problem, program, or service is important to it. What to do may be phrased as a more subtle "request" such as asking someone to look at something differently. The what to do element is the foundation of the triangle, as – in answering this component – your organization makes its message relevant to audiences, based on your correct analysis of what it is and what it means to them.

Step 5, complete a QI check: examine language and symbols. In Step 5, you check your verbal communication; you look at what you've written: your language, the emotions it invokes, and the symbology it conveys. "It is important that messages be truthful as well as clear, persuasive, and concise. The language we use conveys more than the simple meaning of the words. Language suggests the images that will be used to convey our messages. Some words trigger an emotional response, while others convey the need for a more rational approach. Note that some words may bring about a positive feeling in some audiences while at the same time conjuring up negative or uncomfortable emotions in others. ... Get rid of words that have been overused or that have no emotional punch, words that we have come to rely on too much: *services, programs, unique, innovative, facilitate, comprehensive*. Never underestimate the power of symbolic language to convey the emotional context and the values that we want

to have connected to our messages and our missions. ... By connecting the right symbols and values to your cause, issue, or concern, and associating them truthfully with your objectives, you can not only solidify existing support but also win converts to your position.” (Radtke)

Symbolic-language words = *freedom, oppression, privacy, deceit, equality, greed, individualism, dependency, fairness, favoritism, security, suspicion, family, fraud, opportunity, problem, honesty.*

These are examples of jargon to “translate” into plain English: *intervention* (plain English: help, counsel), *facilitate* (bring together), *assessment* (study). As military language is chock-full of jargon, there are many other examples.

“Finally, go through your messages once more and see whether you can simplify the language so that your audience understands exactly what you are saying without your having to explain what you mean. Ideally, someone with an **eighth-grade reading level** should be able to understand what you’re talking about and what you mean.” (Radtke)

Step 6, let go of the message. One, you truly do not have control of the message, and two, your organizational members will be your best message-conveyors via their personal use of social media. “Empower” them to state your message in their social-networking engagements.³⁷⁹ So:

- Once you have made sure that all personnel affiliated with your organization know what the messages are, can say them in their own words, and understand the importance of sticking to the central idea inherent in those messages, let them go out and “engage” in the social-media sphere.
- Drive traffic to any electronic media your organization produces – newsletters, brochures, videotapes, Websites, and so on – which should repeat and reinforce your messages. The necessary step of Step 6 is to ensure you are consistent and provide a headquarters (central) resource; as a headquarters, it will benefit you strategically to be consistent in your Website messages.

Rather conspicuously absent from Web content up to this time have been the *what it means* and especially the *what to do* aspects, which would contribute to making our content more relevant. Building TRADOC messages on the message triangle will help content providers understand what elements are critical. Relevance will also encourage our unofficial bloggers, for instance, to dialogue with members of the American public.

Our messages must be credible to have the greatest impact on the behavioral goals and objectives we have in mind for our stakeholders. “The more personal the communicating, the more important the credibility factor,” say the communications experts. “The more credibility, the more likely the targeted public is to receive, accept, and act on your message.” (Caywood) Thus one of the ways social media can aid our communication – and one of the ways it can massively backfire. However, in personal communication, we can bank on the CG’s credibility as an Army senior leader and the commander responsible for training the current force and building the future force. We need other TRADOC spokespersons in Web content to be just as credible.

Corporate ethos.³⁸⁰ As in the corporate world, TRADOC and its “products” must be reflected on our Websites. But we go one step farther here, and that’s in “branding” our Websites. This notion is actually established in Army policy – it’s not just a marketing term.

“‘Branding’ identifies the organization and creates or enhances positive feelings about it. A successful brand has a high position, or distinctive net impression, in the minds of key publics.” (Caywood)

“Stewardship embraces the creation and maintenance of a good reputation and then builds on it.” (Caywood)

³⁷⁹ IAW Paragraph 3-1e, AR 5-1: “Empowerment shares control, responsibility, and ownership of organizational processes. Empowerment is based on open dialogue, shared purpose and vision, and clearly understood goals and priorities. Empowered employees are focused on providing value to their customers, not on simply completing assigned tasks.”

³⁸⁰ *Corporate ethos* is built on these factors: self-regulation of conduct, transparent relations with society, dialogue and participation with employees / respect for the individual / respect for workers (decent pay for decent work), management of environmental impact, responsibility for future generations, selection and partnership with suppliers (if commercial firm, but apply this to the American public in TRADOC’s case), relations with local community, philanthropy / social investments, volunteer work, political transparency, and social leadership, according to the Ethos Institute for Business and Social Responsibility, http://www.ethos.org.br/_Rainbow/Documents/indicators_2003.pdf.

DA PAM 25-1-1, Paragraph 8-1i, establishes a requirement for corporate sponsorship by requiring that 1) the phrase “U.S. Army” must be clearly displayed on every page, along with organization’s official name, and 2) there must be a statement that the Website contains official government information. This helps establish an organizational identity, also called a corporate ethos.

We establish clear “branding” on our Websites, however, not just by stamping “U.S. Army” and “This is official government information” on them, but also by robustness of content, expressed in language easily understood, posted on Webpages that are not only eye-catching but easily navigated and memorable. “Branding” and an organizational Website should be inextricably linked.

Therefore branding is a Website strategy. The Web is a key information tool as well as a strategic-communication venue, where the CG’s top concerns and topics can be emphasized merely by a presence on the TRADOC homepage. Successfully branding a Website is inherent in the following criteria, which should be **assessed yearly for effectiveness**:

- Ease and consistency of use / navigability;
- Key messages conveyed;
- Interactivity;
- Consistent content;
- Integration with the rest of TRADOC’s information products.

Branding TRADOC’s Websites supplements the enhancement of TRADOC’s corporate ethos and reputation. Branding helps build support for the organization’s mission, principles, and objectives; and keeps, or stewards, the organization’s reputation as it influences the actions of groups who are key to the organization’s success (based on Caywood).

The Web is important to TRADOC’s corporate ethos because it allows establishment of consistent corporate content (corporate cohesion), reaching across a broadly diverse audience. Using the Web, the HQ may:

- Speak with “one voice.”
 - Employing “one voice” enables the organization to unanimously, consistently describe how it is fulfilling its role in supporting an Army and country at war and / or supporting TRADOC’s communication objectives as described by TRADOC strategic-communication messaging or PAO content guidance.
- Make available consistent statements of the CG’s mission, vision, goals, priorities, and policies, which all TRADOC sites should support with content.
- Ensure that all organizations outline strategic-communication points and their role in them.
 - Standardize and make consistent TRADOC’s message.
 - Show how TRADOC is the Army’s lead change agent.
 - Enhance understanding of TRADOC’s role in supporting the Army.
 - Advance a key set of ideas on behalf of the Army.

As we work toward relevant messaging, branding, and corporate ethos at HQ TRADOC, we should have several near-term goals, then some longer-range goals:

- Near-term goals for content:
 - Establish content supporting TRADOC communication objectives.
 - The goal is that TRADOC’s communication objectives show how TRADOC is supporting the Army’s strategic-communication priorities, and in synch with that, organizational communication objectives show how organizations support TRADOC’s communication objectives.
 - Establish corporate ethos, building on the corporate Web-design template.
- Longer-range goals for content:
 - TRADOC’s site to be the Website of choice for the Army, since “if it’s happening in the Army, it’s happening here.”

- “One voice” *and* relevant content built on the message-triangle concept. At this point, we’ll have progressed a long way in offering valuable information of interest to the general public and in telling TRADOC’s story.

As a corporate entity, TRADOC is fragmented in how successfully we communicate the importance of what we’re doing for the Army and for the nation. And we’re not saying these things as a starry-eyed marketing major fresh out of college. The Army has been “boots on the ground” at war since 2001. The propensity for military service (and those qualified to do it) has declined. The American public is not only jaded about the war on terrorism, but there is a rising trend of disbelieving there is any terrorism threat. Spurred by constant stories of alcoholism among Soldiers, perceived rising domestic abuse / rising violence / rising sexual abuse / rising suicide rates, the Army appears “broke.” We are therefore at no more critical time, and with no more critical mission, than to responsibly engage on ways the Army is addressing its corporate ethos – especially with respect to conduct and values self-regulation, relations with and reliance on the American public, respect for each individual, and our care-taking for the future – and so we are *obligated* to strive for corporate cohesion via branding and other techniques.

Therefore, as the content required by DA PAM 25-1-1 is put in place, and as we begin to think in terms of strategic Web content, Web-content reviews should begin to include scrubs on corporate cohesion and corporate branding.

PUBLIC ACCESSIBILITY AND WEB SECURITY

Chapter 1 discussed the public domain as framed by network and IA regulations (AR 25-1 and 25-2), defining *publicly accessible* as Webpages on which there is no security or access control. Since what the public can access is determined by network controls, that’s within the Web-content manager’s concerns. Therefore this section of Chapter 4 will go into more detail, defining *public accessibility*, providing DoD policy for the security and access controls that must be given to content prohibited on the publicly accessible Web, and providing a framework for the concept of zero-based content mentioned in Chapter 1.

In a nutshell, DoD and Army policy determines releasability of information on the WWW based on whether the information’s target delivery venue is a Website in the public or in the non-public domain – i.e., whether the Website does not authenticate individual users or restricts access solely by domain or IP address (public), or whether it authenticates individual users (non-public). Access control defines the difference between *publicly accessible* and *non-publicly accessible* when it comes to the Web, and therefore the difference between *public domain* and *non-public domain*. Control must be, at minimum, a “positive” access control such as a user ID and authenticator: AKO authentication, Common Access Card (CAC) authentication, and / or restriction by user name / password. Recommended access control is via CAC log-in. These requirements are discussed further, following.

Public accessibility can be amorphous, given shape only by understanding key principles from DoD and Army policy and guidance. These principles, for purposes of this *Guide*, come under the generic headings of “content” and “security.” Policy is given per principle listed.

The principles of content. The WWW was not designed with security in mind. It was designed to share information. The “locks” on information access come when content providers ask themselves, “Why does the WWW public need to know this?” and emphasize that access to the WWW is worldwide. The worldwide access is why DoD defines rules for what should and should not go on a Website as part of its focus on “content security” for material that is published on public Websites. DoD also defines how information should be reviewed before it is posted to a Website; in general, DoD policy and Army policy state that all material will be reviewed prior to posting to a DoD Website, as well as quarterly thereafter.³⁸¹ This is discussed in detail in previous chapters.

Following are some principles of content for public Websites (other principles are outlined in previous chapters):

- Public sites are developed when an organization wishes to provide *all* users with information.³⁸²
- WWW users are encouraged to access public sites as their preferred and routine choice to research or develop and exchange information.³⁸³
- Public Websites are on the Internet (WWW) and are considered unrestricted.³⁸⁴

³⁸¹ Paragraphs 1.3.3 and 2, Part V, DoD Web policy; Paragraph 2-3a(15), AR 530-1; Paragraphs 3-3i, 4-5a(7), and 4-20g(11), AR 25-2; Paragraph 6-7c(3) and (4), AR 25-1; Paragraph 8-2b(3), DA PAM 25-1-1.

³⁸² Paragraph 5-5c, TR 25-1.

³⁸³ Paragraph 6-4n, AR 25-1.

³⁸⁴ Paragraph 6-7a(7), AR 25-1.

On the other hand, private sites are developed when the Website's target audience is specific and exclusive. These are the principles of content for private Websites:

- Website owners must establish appropriate mechanisms to protect sensitive information. Access to content on the private side is authorized according to how those controls are applied.³⁸⁵
- Not all content is appropriate for the publicly accessible Web. Determinations as to whether the content should be public or non-public will be based upon 1) the sensitivity of the information, 2) the target audience for which the information is intended, and 3) the level of risk to DoD interests, which will be determined by an OPSEC assessment.³⁸⁶ Content providers / content reviewers must consider these elements in matching information types to what security and access controls to employ IAW Table 1, Part V, of the DoD Web policy.³⁸⁷
 - Table 1, Part V, of the DoD Web policy provides the types of information and the security and access control appropriate to its type. In essence, only information of interest to the general public should be on "open" Webpages – pages that have no access control. The vulnerability of Webpages that have as an access control a restriction by Internet domain (e.g., .com, .edu, .org, .mil, .gov) or IP address is *very high*. The vulnerability of Webpages with access control of limitation by user ID and common password is *high*. Even AKO is at risk, as adversaries may compromise login credentials (username and password), based on credential thefts over the past couple of years, and can exploit improper content-access settings with those stolen credentials to obtain sensitive information.³⁸⁸ An organization can post FOUO information or information sensitive by aggregation only when it employs PKI software or hardware tokens for access to its content, IAW DoD Web policy.
- Information included in the following categories may not be accessible to the general public: FOUO information; information not specifically cleared and marked as approved for public release IAW DoDD 5230.9 and DoDI 5230.29; or information of questionable value to the general public and for which worldwide dissemination poses an unacceptable risk to DoD, especially in electronically aggregated form. Information in these categories must employ positive security and access controls appropriate to the type of information.³⁸⁹

Even the Internet (publicly accessible side), when a user is on a government-owned computer, employs some minimal security. At minimum, a "notice and consent banner" activates as a user logs onto the IS – including, but not limited to, access to the Web, FTP, telnet, or other services.³⁹⁰ The IS typically advises DoD telecommunications systems / devices users that the systems / devices are for authorized use; that they are subject to monitoring, including their personal communications and stored information; that using government telecomm systems / devices constitutes the user's consent to monitoring; and that users may expect no privacy while using ISs or accessing Army resources.

The principles of security. Web security can be described as a moving target – thus the layers of DoD and Army policies and guidance. Policies concerning Army Web policy and publicly accessible Websites – the "rules" – include the Americans with Disabilities Act, export laws, FOIA, PRA, Privacy Act, Telecommunications Act, DoD Web policy, FOUO regulations, DoD 5500.7-R (the JER), DoDI 5120.4, DoDD 5122.5, DoDD 5230.9, DoDI 5230.29, AR 360-1, AR 25-2, AR 530-1, AR 25-1, DA PAM 25-1-1, et al.

(*Guidance* is the subsequent information issued that personnel take into account to correctly implement policy, like this user guide and information contained on the TRADOC WCWG portal. As mentioned at the beginning of Chapter 1, TRADOC organizations with Webpages, portals, repositories, and shared drives can adhere to the

³⁸⁵ Paragraph 6-4n, AR 25-1.

³⁸⁶ Paragraph 3.6.2, Part II, DoD Web policy. Also see Table 1, Part V, DoD Web policy.

³⁸⁷ Paragraph 5-3b, TR 25-1.

³⁸⁸ ALARACT 089/2008, "Securing AKO Content and Credentials (NIPR)," March 25, 2008. User login credentials may be stolen from a user's home, office, or public Internet-access locations. Malicious software to capture user logins and other information may be installed on a user's computer without his / her knowledge via programs like chat, file sharing, and free downloads from untrusted sites.

³⁸⁹ Paragraph 4.3.1, Part I, DoD Web policy. Also see Paragraph 2, Part V, DoD Web policy. Cited in message posted to 5th Signal Command Webmasters listserver March 5, 2003, by the chief of the Vulnerability Assessment Division (VAD), 1st IOC.

³⁹⁰ Paragraph 4-5m, AR 25-2.

policies and principles in this *Guide* to maximize the security and accessibility of their content,³⁹¹ as this *Guide* is based on DoD and Army policy and guidance.)

These categories are considered **publicly accessible** simply because no security / access control is applied, or it is inadequate:

- Websites posted on a **.mil domain** or other domain without access control, and whose content makes them official Websites (includes .edu, .gov., .com).
- A Website using **SSL restriction**. SSL, a data-transport protocol, works by combining programs and encryption / decryption routines existing on the Web-hosting computer and in the user's browser. Therefore SSL only authenticates the server, while the client / user remains unauthenticated. (PKI is the only thing that authenticates both server and client / user.) **Hypertext Transfer Protocol-Secure (HTTPS)**, which some military Websites use as pseudo-security, **is publicly accessible**. The "s" at the end of Hypertext Transfer Protocol (HTTP) merely means that a Website visitor has established an SSL session through the HTTPS-secured URL.
- A Website using a **single password for all users**. A common password is not an adequate authenticator.
- A Website that **does not authenticate** individual users.³⁹²
- A Website that employs only **domain or IP restriction as access restriction**.³⁹³ The IP address is a unique number that identifies each machine on the Internet – nicknamed "dotted quad" because the IP consists of four sets of numbers between 0 and 255 separated by dots / periods. The IP address points to the domain, which is tied to a name server – the number is "translated" into a name, such as www.tradoc.army.mil. Thus a Webpage can be restricted from access by those not having the approved domain / IP. Because of this method's age (the Army first used it in 1997), domain and IP restriction are not secure and therefore are in the realm of publicly accessible.
- A TRADOC AKO organizational **portal**³⁹⁴ and any **KCs** within that portal that have **"open" access permissions**.
- An **FTP site**. FTP operates with authentication but without encryption, so although its administration can be run through secure shell, FTP data is still open to sniffing and attack. FTP sites in the public domain are not authorized and may not be used in place of authorized public Websites.³⁹⁵

Because separation between the NIPRNET and the WWW is ambiguous, unencrypted information on the NIPRNET is at risk for compromise by an adversary or competitor. Servers must employ a combination of access and security controls on the NIPRNET for content intended for internal DoD use only, as this information is likely to be accessible to non-DoD users without the access control.³⁹⁶ Controls may include firewalls, routers, or host-based systems to ensure the integrity, confidentiality, accessibility, and availability of DoD ISs and data.³⁹⁷

Following are principles of security for the NIPRNET:

- **All servers, including Webservers**, that are connected to publicly accessible computer networks such as the Internet **will be configured to employ access and security controls** (e.g., firewalls and routers) to ensure integrity, confidentiality, accessibility, availability, non-repudiation, and authentication, **regardless of classification level** of DoD ISs and data.³⁹⁸
- **All non-public Web content must be on a site that is accessible only through methods that authenticate the individual client / user** – in other words, the site uses *positive security and access control*.³⁹⁹ Positive security and access controls are those which authenticate individual client / user access; Army IA policy on

³⁹¹ Paragraph 5-3, TR 25-1.

³⁹² ALDODACT message 11/06.

³⁹³ ALDODACT message 11/06; memorandum from the ASD-C3I, "Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites," Dec. 28, 2001; Paragraphs 6-7a(7) and 6-7e, AR 25-1; Paragraph 5-5d, TR 25-1; message posted to the 5th Signal Command Webmasters listserver March 5, 2003, by the chief of VAD, 1st IOC.

³⁹⁴ Paragraph 5-5c, TR 25-1.

³⁹⁵ Paragraph 6-7a(10), AR 25-1.

³⁹⁶ Paragraph 1.3.2, Part V, DoD Web policy.

³⁹⁷ Paragraph 4-20g(10), AR 25-2.

³⁹⁸ Paragraphs 4-20a and 4-20g(10), AR 25-2.

³⁹⁹ Paragraph 4-5c(7), AR 25-2. Also see Paragraph 3-4c, DA PAM 25-1-1, and Paragraph 5-3a(4)(d), TR 25-1.

access controls are a minimum of user ID and an authenticator. (The password is the most common authenticator but isn't necessarily the one Web managers should be applying – see the following principles.) An *authenticator* is something the user knows, such as a unique password; something the user possesses, such as a token (CAC card); or a physical characteristic (biometric).

- Authenticators such as PKI and biometrics are called *IA-enabling technologies* and will be used to enhance information protection.⁴⁰⁰
- ISs must identify users through the user's use of unique user IDs.⁴⁰¹
- Commanders must validate that systems authenticate users through the use of the CAC as a two-factor authentication mechanism.⁴⁰² The CAC will be used as the primary user identifier and access authenticator to systems. The CAC is the primary token for both Class 3 and target Class 4 PKI certificates used in unclassified environments for active-duty military personnel, members of the Selected Reserve, DoD civilian employees, and eligible contractors.⁴⁰³
- Class 3 PKI is the minimum DoD-wide standard for client / user authentication.⁴⁰⁴
- Unpublished Web addresses (URLs) and unlinked Webpages stored on the Webserver do not provide security.⁴⁰⁵
- Working-draft content must not be stored in publicly accessible files or portals.⁴⁰⁶
- Publicly accessible Army Websites may provide hyperlinks to access-controlled Websites only through intervening access-control mechanisms or procedures sufficient to address the perceived level of threat and sensitivity of the information.⁴⁰⁷
- FOUO information can only be posted to a site that, at a minimum uses SSL for transmission control and PKI at the software or hardware level for access control.⁴⁰⁸
- Web applications must be PKI-enabled.⁴⁰⁹
- Organizations that collect SBU from the general public as part of their assigned mission may buy and use approved commercially available certificates to provide SSL services for ease of access.⁴¹⁰

Beyond working with the network manager to ensure that any private Website is secured by the proper authenticator, Web-content managers do not have to worry about the server's security like the Web manager does. However, it may be useful for Web-content managers to know some more of the security measures a Web manager must take:

- Network managers must protect publicly accessible Army Websites by placing them behind a reverse Web proxy server. The reverse proxy server acts as a proxy from the intranet to the protected server, brokering service requests on behalf of the external user or server. This use of a reverse proxy server provides a layer of protection against Webpage defacements by preventing direct connections to Army Webservers.⁴¹¹ Reverse proxy servers must be configured in a way that does not cache SSL traffic.⁴¹²
- Publicly accessible Websites *not* protected behind a reverse Web proxy (until moved to the reverse Web proxy) will be on a dedicated server in a *demilitarized zone* (DMZ), with all unnecessary services,

⁴⁰⁰ Paragraph 5-1c, AR 25-1.

⁴⁰¹ Paragraph 4-5c(5), AR 25-2.

⁴⁰² Paragraph 4-5c(6), AR 25-2.

⁴⁰³ Memo from the DoD CIO, "Department of Defense (DoD) Public Key Infrastructure (PKI)," Aug. 12, 2000.

⁴⁰⁴ Memo from the DoD CIO, "Public Key Enabling (PKE) of Applications, Webservers and Networks for the Department of Defense (DoD)," May 17, 2001; memo from the DoD CIO, "Department of Defense (DoD) Public Key Infrastructure (PKI)," Aug. 12, 2000.

⁴⁰⁵ SECDEF message, "Website OPSEC Discrepancies," Jan. 14, 2003.

⁴⁰⁶ Paragraph 5-3b, TR 25-1.

⁴⁰⁷ Memorandum from DISC4, "Guidance for Management of Publicly Accessible U.S. Army Websites," Nov. 30, 1998.

⁴⁰⁸ Table 1, Part V, DoD Web policy. 1st IOC uses Table 1 in its Web-content reviews, according to a message posted on the 5th Signal Command Webmasters listserver March 5, 2003, by the chief of VAD, 1st IOC. PKI is required of FOUO information; SSL is required of private servers.

⁴⁰⁹ Paragraph 6-7e(4), AR 25-1.

⁴¹⁰ Paragraph 6-7e(6), AR 25-1.

⁴¹¹ Paragraph 4-20g(12), AR 25-2; Paragraph 6-7c(6)(a), AR 25-1.

⁴¹² Paragraph 6-7c(6)(a), AR 25-1.

processes, or protocols disabled or removed. Supporting Regional Computer Emergency Response Teams (RCERTs) and Theater Network Operations and Security Centers (TNOSCs) conduct periodic vulnerability assessments on all public servers and may direct that a Website be blocked, depending on the inherent risk of identified vulnerabilities – thus the possible sudden changes and blocks on public content.⁴¹³

- Network managers must ensure that they do not install or run publicly accessible Websites under a privileged-level account on any Webserver, since with a privileged-level account, programs can be downloaded and executed without the user knowing. Similar configuration for non-public Webservers, unless they're operationally **required** to run as a privileged account and unless appropriate risk-mitigation procedures have been implemented.⁴¹⁴ Someone with a privileged-level account has administrative or elevated rights on their computer or on the network.
- Webservers that are externally accessed (publicly accessible) must be isolated from the organization's internal network. The isolation may be physical, or it may be implemented by technical means such as an approved firewall. In cases where an organization operating a TRADOC Website determines a requirement to host both a public and non-public Webserver, additional security measures are required for the private Webserver. At minimum, appropriate access controls, audit of security events, and additional measures to ensure confidentiality, integrity, and availability of the information must be employed.⁴¹⁵
- Network managers must enable all unclassified intranets (private Websites used for processing information limited to DoD users) to use DoD PKI certificates for server authentication and client / server authentication. Owners of authorized intranets must ensure that SSL is enabled and PKI encryption certificates are loaded.⁴¹⁶
- An unclassified, private Webserver is exempt from using CAC / PKI or other forms of encryption only if it meets one of these three conditions:⁴¹⁷
 - Provides non-sensitive and publicly releasable information resources, but is categorized as a private Webserver because it limits access to a particular audience only for the purpose of preserving copyright protection of the contained information sources;
 - Facilitates its own development; or
 - Restricts access to link(s) to limited access site(s) (and not the information resources).

All Army private (non-publicly accessible) Websites must be located on a .mil domain.⁴¹⁸ In fact, all TRADOC public and private Websites must be on the .mil domain, except those operating under the Army Accessions Command's Integrated Automation Architecture (AAC-IAA)⁴¹⁹ or unless a waiver is approved by the Army G-6. (No waiver needed if the entity is one of the exceptions granted in Enclosure 3, DoDI 8410.1.) **Pre-existing Army Websites maintained in non-government domains (i.e., .org, .com, .net and .edu) not falling under DoDI 8410.1's exceptions must transition to the .mil domain.**⁴²⁰ Regardless of the current domain, Army Websites are official Websites because of their content (see definitions section, this **Guide**) and must comply with all federal, DoD, Army, and TRADOC Webserver and Web-content policies and guidance.

AKO / DKO offers its own set of concerns vis a vis whether the content is in an unrestricted or restricted area. Some of the preceding principles covering authentication requirements should help shed some light. The NIPRNET side of AKO is authorized for content up to unclassified / FOUO or CUI.⁴²¹ However, *basic AKO authentication* at this stage of technology isn't sufficient for posting FOUO information because AKO accounts can be held by individuals not authorized FOUO access.⁴²² If FOUO is to be posted on AKO, additional / secondary checks of user credentials are required to ensure appropriate user authentication, including entry of an additional password / ID.⁴²³

⁴¹³ Paragraph 4-20g(13), AR 25-2.

⁴¹⁴ Paragraph 4-20g(5), AR 25-2.

⁴¹⁵ Paragraphs 5.3 and 5.5, Part II, DoD Web policy.

⁴¹⁶ Memo from the DoD CIO, "Department of Defense (DoD) Public Key Infrastructure (PKI)," Aug. 12, 2000; Paragraph 6-7e(2), AR 25-1; Paragraph 4-20g(14), AR 25-2.

⁴¹⁷ Paragraph 6-7e(5), AR 25-1.

⁴¹⁸ Paragraph 6-7b(1), AR 25-1; Paragraph 4, DoDI 8410.1.

⁴¹⁹ Paragraph 5-5, TR 25-1; Paragraph 4 and Enclosure 3, DoDI 8410.1.

⁴²⁰ Paragraph 5-5, TR 25-1; Paragraph 4 and Enclosure 3, DoDI 8410.1.

⁴²¹ ALARACT 089/2008, "Securing AKO Content and Credentials (NIPR)," March 25, 2008.

⁴²² Paragraphs 3-4c and 3-4d, DA PAM 25-1-1.

⁴²³ IAW message posted on the 5th Signal Command Webmasters listserver March 5, 2003, by the chief of VAD, 1st IOC.

The unrestricted area of AKO (available to all users, not further access controlled), which is required to have PAO content review, isn't sufficient security and access control for FOUO information.⁴²⁴ AKO authentication is based on employment status and is done by means of active Army or DoD databases, such as secure Lightweight Directory Access Protocol (LDAP), the Integrated Total Army Personnel Database (ITAPDB), or the Defense Enrollment Eligibility Reporting System (DEERS) – therefore the validation is based on information that may or may not be current, and on a status that may or may not be current. Further, although the Army uses LDAP to authenticate clients, the Army is moving away from LDAP; now all intranet Web applications must use AKO single-sign-on (SSO) or AKO SSO with CAC for user access, unless waived. Legacy applications currently using AKO / DKO LDAP to authenticate clients must migrate to SSO-capable platforms.⁴²⁵ Because of technological changes, at some point in near-future time, PAO review anywhere on AKO may not be required, but that currently isn't the case.

Also, due to the possible theft of login credentials,⁴²⁶ an adversary may be able to access AKO's unrestricted area. Therefore, in determining access controls on AKO NIPR, personnel should consider risk mitigation and the possibility that unclassified or FOUO / CUI information may become sensitive, or even classified, in the aggregate.⁴²⁷ Since the primary content repository within AKO is the KC,⁴²⁸ and since Army and TRADOC policy require TRADOC organizations to use AKO KCs for non-public content, network managers can employ a positive access control beyond basic AKO authentication for access to this content to meet the requirements. Or, network managers can use other approved TRADOC options for restricted-access portals such as AKO team sites, TKE, or BCKS.⁴²⁹

As a sidebar note, all AKO / DKO account users are responsible for securing their AKO / DKO credentials (i.e., user name and password). Also, the Army prefers CAC logon to user name and password logon.⁴³⁰

AKO / DKO is the single authoritative source for authenticating user access to Army Web-enabled ISs and Webservers that serve users with DoD IP addresses.⁴³¹ Activities must therefore use AKO and AKO-Secret portals as the primary tools for collaboration. Existing Army portals or Webservers with authentication services that duplicate AKO / DKO services must migrate to AKO / DKO authentication unless CIO / G-6 waives this. Further, Army Web-enabled business applications must be linked from the AKO / DKO portal. The initial minimum standard is a URL link on the Army portal to the application, while the objective standard is to use AKO / DKO directory services for authentication as well as a URL link on the Army portal.

While not permitted to be general-public accessible, where collaboration with non-DoD personnel regarding unclassified official information will benefit DoD, official "chat rooms" or collaboration sites may be established. These collaboration sites must be regulated through the use of positive technical controls such as proxy services and screened subnets IAW DoDI 8500.2, **Information Assurance (IA) Implementation**, and approved by the DoD designated approving authority (DAA).⁴³² Collaboration can take place among DoD personnel, or among DoD personnel and authorized non-DoD personnel (including public members of the scientific community), within security and information dissemination guidelines (for example, export control restrictions). Non-DoD personnel must be authorized access to the "chat room" or collaboration site on a by-name basis by the DoD sponsor IAW procedures established by the DAA. Client / user authentication is required for system access.⁴³³

⁴²⁴ Paragraph 6-7d(4), AR 25-1.

⁴²⁵ Paragraph 6-7e(3), AR 25-1.

⁴²⁶ ALARACT 089/2008, "Securing AKO Content and Credentials (NIPR)," March 25, 2008.

⁴²⁷ Ibid.

⁴²⁸ Paragraph 3-8a, DA PAM 25-1-1. AKO allows the user, community, or team to create KCs or personal team areas available from any Internet connection. The KC allows the user, based on the type of user account, to upload and download files, share files, subscribe to working-team content, control versions, and delete files. The KC site administrator maintains the rules for reference posting, versioning, and archiving of content. The KC has AKO-defined roles and rules for maintenance and archiving. Content roles allow the user access to content based on applied rules such as account type, access level, and specific site restrictions. See Paragraph 3-8b of DA PAM 25-1-1 for user types / access levels.

⁴²⁹ Paragraph 5-5d, TR 25-1.

⁴³⁰ Paragraph 6-7d(5), AR 25-1.

⁴³¹ Paragraph 6-7d(2), AR 25-1.

⁴³² Consult TRADOC G-6 – see Paragraph 1-5a(10), TR 25-1.

⁴³³ ALDODACT message 11/06.

The zero-based approach to Web content.⁴³⁴ The zero-based approach to Web content (mentioned in Chapter 1) integrates both the principles of content and security. These are the most important considerations (and benchmarks) in zero-based Website security:

- Assess the benefits to be gained by posting specific types of information on a Website. Identify a target audience for each type of information and why their need for the information is important to the organization's mission. A careful examination of the potential consequences of placing information on the Website is necessary. (See the DoD Webmaster policy, Paragraph 3.1 in Part II.)
- Post only information for which the organization is responsible. Since any organization knows its own critical information best, it can reduce the vulnerability of other organizations by letting them post their own information. (See the DoD Web policy, Part II, Paragraph 2.3, and the policy on duplication of content later in this chapter.)
- Do not post public links to sensitive sites. These links identify the existence and location of potential targets for an information collector who may previously been unaware of them. If it is necessary to link to sensitive sites, the link should pass through an intermediate site, which can screen visitors through passwords or other criteria. (See the DoD Web policy, Part II, Paragraph 3.6.3.)

The zero-based approach to Web content is recommended because once the information is posted to the Web, it cannot be retracted, so it must be protected prior to dissemination.⁴³⁵ There are a number of Website / Webpage archiving sites that ensure that, even if information is removed, it is still available to researchers, including adversaries.

Our adversaries' ability to aggregate information from open sources, especially the Internet, is often underappreciated. The United States faces cunning and ruthless adversaries fighting asymmetrically to avoid our strengths. The first step for them to inflict harm is to gather information about us. They exploit the openness and freedoms of our society by aggressively reading and collecting material that is needlessly exposed to them. In fact, the adversaries' asymmetric methods of warfare strongly emphasize collecting information from unclassified and open sources. As a result, many adversaries do not need to invest in costly and highly technical intelligence collection systems when they can obtain as much as 80 percent to 95 percent of the information they are seeking openly and legally.⁴³⁶

In recent years, in fact, the Internet has become an ever-greater source of open-source information for U.S. adversaries – in particular, individual Soldiers and Soldiers' family members' personal Websites (including blogs) are a potentially significant vulnerability, according to AR 530-1. Other sources for open-source information include public presentations, news releases from units or installations, organizational newsletters (both for official organizations and unofficial organizations, such as alumni or spouse support groups), and direct observation.

Controlling vulnerabilities at the source – our voluntary release of information – should help this situation.⁴³⁷ AWRAC scrubs performed between January 2006 and January 2007, as reported in commercial media in August 2007, found more than 1,800 OPSEC violations on 878 official military Websites. For instance, AWRAC's audits found a map of an Army training center and a spouse's maiden name (prohibited PII).

"E-gov isn't easy in a Webscape dotted with YouTube, Wikipedia, blogs, and changing expectations. ... According to the University of Michigan's American Customer Satisfaction Index, the government is behind in matching the increasing popularity of social networking and user-generated content." – Stephen Barr, "Public less satisfied with government Websites," posted at washingtonpost.com, March 21, 2007

SOCIAL MEDIA

One of the most controversial uses of the publicly accessible Web is

⁴³⁴ Adapted from the *IOSS Intelligence Threat Handbook*.

⁴³⁵ Paragraph 1-7a(3), AR 530-1.

⁴³⁶ Paragraphs 1-7b and E-1c, AR 530-1.

⁴³⁷ Paragraph E-3a(2)(b), AR 530-1.

DoD's engagement in social media.⁴³⁸ A PAO trying to research what is permissible under the regulations will feel like he / she has hit a number of brick walls, since the argument on social media has been framed by ARs under the IRM / IT / IA umbrella, while Public Affairs has lagged in producing policy or even minimal Public Affairs guidance (PAG). **Army leaders such as Secretary of the Army Pete Geren have said that Public Affairs must engage**

Federal agencies don't have a reputation for being hip when it comes to Internet outreach, but more government leaders are starting to see the upside of using social media to deliver their messages and connect with taxpayers. ... A quick scan of the Web shows that agencies are going outside their comfort zone to disseminate information across a range of platforms. While getting on board with these new-media tools has taken a culture change, agency leaders have begun to realize that when citizens search for information from the government, they want to use the same avenues they do in their everyday lives." – Elizabeth Newell, "Agencies test new waters in social media," govexec.com, Feb. 19, 2009

in social-media venues. (See Geren's statement, Page 161.)

DoD-level representatives consider the use of social media integral to national security.⁴³⁹

And we know that social media are "where the people are" – especially since, in today's busy world, social media is portable to people's portable electronic devices (PEDs) such as cellphones, pagers, personal digital assistants (PDAs) (e.g., Palm Pilots and Pocket PCs), laptops, memory sticks, thumb drives, and two-way radios.⁴⁴⁰ However, everywhere an Army PAO turns, the answer seems to be "no" on permission to use social media. And so the practice is to use social media anyway, as it seems easier to ask forgiveness than to get permission.

To add difficulty to the situation, Army Public Affairs blithely advises Army personnel to "go forth and blog" without appearing to wrestle with the issues "the field" does. So what's a PAO at ACOM level and below to do?

Let's look at the existing policy and at what's coming in the future.

Brick wall #1: Social-media usage and monitoring aren't stated authorized uses of government telecommunications systems. Social-media engagement must adhere to DoD and Army policy on official and authorized use of telecommunications.⁴⁴¹ Authorized and prohibited uses of telecommunications are outlined in Paragraphs 6-1e and 6-1f, AR 25-1. Use of telecommunications, including computers, must be IAW legitimate public interest and may not adversely affect performance of official duties by the employee or employee's organization; may not adversely reflect on DoD or the Army; may not be uses that are incompatible with public service; must

be of reasonable duration (normally five minutes or less) and frequency (twice per day), and, whenever possible, are made during the employee's personal time, such as during lunch, break, and other off-duty periods; are not used for activities related to operating a private business enterprise; may not be for unlawful activities, commercial purposes,

⁴³⁸ Social media refers to dialogue-based Web platforms, including sites such as Facebook, MySpace, Flickr, YouTube, and Twitter.

⁴³⁹ For instance: "This is not just techie-geeky stuff, but serious stuff with national security ramifications. We can't ignore [social media] if other nations are using it, both friends and adversaries. If the government keeps not making use of these technologies, we'll fall behind and be unaware of things that could affect us." – Linton Wells, distinguished research professor at National Defense University (NDU), former DoD CIO, and co-author of a policy paper, along with NDU associate research fellow Mark Drapeau. The policy paper examines how software applications that allow groups of people to connect and communicate on-line affects government security and how DoD should use social media in its operations. "If you work in national security, some of these things happening in other countries may affect your job or mission. What's happening over the past couple years is people in other countries are using Facebook, Twitter, and blogs to organize. In some cases, even when government security knew it was happening, they were overwhelmed by the amount of people who showed up." – Mark Drapeau. "Not being involved [with social media] is probably a greater risk than anything you may encounter from being involved. Listening to public conversations and adjusting policies based on what is learned would prevent larger controversies and backlashes against the United States." – Jack Holt, senior strategist for emerging media at DoD. Holt says that not monitoring international dialogues on social-media sites to identify potential conflicts is more risky than any adverse consequences that may occur if employees are allowed to use the tools. All three men are quoted in the article, "Researchers say social media essential for national security," by Gautham Nagesh, April 15, 2009.

⁴⁴⁰ From Paragraph 4-29, AR 25-2.

⁴⁴¹ Paragraph 6-7a(9), AR 25-1.

or in support of for-profit activities, personal financial gain, personal use inconsistent with DoD policy, personal use that promotes a particular religion or faith, or uses that violate other Army policies or laws – this may include, but is not limited to, violation of intellectual property and copyright laws, gambling, support of terrorist or subversive activities, and sexual or other forms of harassment; may not be political transmissions, including transmissions that advocate the election of particular candidates for public office; and may not cause, directly or indirectly, congestion, delay, or disruption of service to any computing facilities or cause unwarranted or unsolicited interference with others' use of communications.

AR 25-2 reiterates DoD policy that federal-government communication systems and equipment (including government-owned Internet systems and commercial systems), when use of such systems and equipment is paid for by the federal government, will be for official use and authorized purposes only. Official use includes emergency communications and communications necessary to carry out the business of the federal government. Authorized purposes include brief communications by employees while they are traveling on government business and can also include limited personal use established by JER guidelines (DoD 5500.7-R).⁴⁴²

The problem here is that some people in the IT world operate under the mindset of “if it’s not specifically authorized, it isn’t authorized.” Also, they argue, social media strays past these parameters: for example, it could adversely reflect on DoD or the Army; it doesn’t stay within the five-minutes-or-less, twice-a-day-or-less duration and frequency guidelines; is not accomplished during the employee’s personal time; or may cause congestion, delay, or disruption of service. This part of Army policy is nebulous enough to cause headaches, as it may be used to buttress other, stronger, prohibitions in AR 25-1.

Brick wall #2: the Army’s blocking / filtering policy. Paragraph 6-1g of AR 25-1 says that Paragraph 4-5, AR 25-2, authorizes use of Web-access blocking / filtering tools for blocking access to “inappropriate” Websites – inappropriate Websites are Websites whose content is the prohibited areas itemized in Paragraph 6-1f, AR 25-1. Although AR 25-1 guarantees that exceptions to the policy will be made for jobs that require “unimpeded access” to the Internet because of mission requirements – listing PAOs, intelligence specialists, SJAs, IGs, auditors, and criminal-investigation specialists – the DOIMs have only recently been organized under the current hierarchy and thus standards have been unevenly applied: some PAOs gained access, some did not. Recently the DOIMs were reorganized – 93rd Signal Brigade, based at Fort Eustis, Va., now has operational control (OPCON) of IMCOM-managed Eastern Region DOIMs, while 106th Signal Brigade, based at Fort Sam Houston, Texas, has OPCON of IMCOM’s Western Region DOIMs.⁴⁴³

The Signal brigades issued operational orders (OPORDs) in mid-May 2009 that directed DOIMs to modify Web-filtering software, allowing access to specific social-media sites. The DOIMs were directed to “support the intent of senior Army leaders to leverage social media as a medium to allow Soldiers to ‘tell the Army story’ and to facilitate the dissemination of strategic, unclassified information,” unblocking “social media sites available from the Army homepage, <http://www.army.mil>.”

The sites now accessible are Facebook, Delicious, Flickr, Twitter, and Vimeo. Still blocked by Joint Task Force-Global Network Operations (JTF-GNO), which is the ultimate authority for what Websites must be blocked on military networks, are YouTube, 1.FM, Pandora, Photobucket, MySpace, Live365, hi5, Metacafe, MTV, BlackPlanet, StupidVideos, and Filecabi, according to the OPORD. The accessibility of social-media sites may change as the sites linked from the Army homepage change.

However, “[a]ccess to prohibited Websites for mission-support reasons is considered authorized use,” according to AR 25-1. Therefore PAOs can still apply for exception to policy using JTF-GNO’s form. A blank form, tips, and samples are available on the OCPA On-line and Social Media Division (OSMD)’s AKO page, <https://www.us.army.mil/suite/page/505262>.

⁴⁴² Paragraph 4-5r(4), (5) and (6), AR 25-2.

⁴⁴³ The 93rd Sig. Bde. and 106th Sig. Bde. are subordinate to 7th Signal Command, Fort Gordon, Ga., which assures network access to Army forces inside CONUS. The 7th Sig. Cmd., a new command (stood up in August 2008), currently has OPCON only over network assets on IMCOM-managed installations and facilities. Therefore the brigade OPORDs, based on guidance from JTF-GNO, affect only installations in CONUS managed by IMCOM. (Network responsibility for installations managed by other commands and activities such as Army Materiel Command and Army Medical Command will come to 7th Sig. Cmd. later.) Prior to issuance of the OPORDs, policies varied about which Websites were accessible on Army networks, but the OPORDs standardized Web access across the command’s area of responsibility. <http://www.army.mil/news/2009/06/12/22553-web-standards-order-opens-some-social-networking-sites-in-conus/?ref=home-ata71-title>.

If these brick walls are hard to get around just to access and monitor social-media sites, what are the brick walls like for actually using social media – to blog, for instance? Again, AR 25-1 and AR 25-2 have set the framework; since all new media is Web-based and publicly accessible, the Web policy and public-release policies are pertinent.

Brick wall #3, blogging is not allowed on Army-owned public Websites. Paragraph 6-7c(4)k, AR 25-1, says it fairly clearly: “Army organizations using the Internet will not post the following types of information on Army’s publicly accessible Websites: ... [blogs], video logs [vlogs], or chat rooms.” The entire regulation drives usage of the Internet toward [army.mil](#), and also requires that official Websites be in compliance with all the various policies of AR 25-1. Thus a Catch-22: you can’t blog on the NIPRNET, and you can’t blog off the NIPRNET (i.e., on a commercial Internet service provider (ISP)). AR 25-1 doesn’t ban blogging entirely, but it sets conditions on blogging – confirmed at the August 2008 TRADOC Public Affairs conference, when G-6 representatives said that G-6 isn’t against blogging in general, but they’re against blogging when it’s done 1) on publicly accessible Websites 2) on the NIPRNET 3) but this doesn’t apply to AKO.

Yes, you can blog on AKO (where it’s considered a social-networking site (SNS)-like service⁴⁴⁴), but you must comply with Paragraph 6-7d(6), AR 25-1: “AKO / DKO users will conform to AKO / DKO posting procedures and policy on the use of official and authorized telecommunications. See [P]aragraphs 6-1d, e, and f.” Same policy as we mentioned in Brick wall #1: IAW Paragraph 6-1d(1), AR 25-1, “The use of DoD and other government ... systems (including the Internet) are limited to the conduct of official business or other authorized uses. [Again, “authorized use” is defined in Paragraph 6-1e, AR 25-1. The JER, Section 2-301, is the basis for the Army’s policy on use of telecommunications and computing systems.]” Usually, no one would “officially” blog something that would seriously “adversely reflect” on DoD or the Army, but the duration and frequency guidelines, plus the fact that AKO blogging most likely would not be done on the employee’s personal time, or the blogging may cause congestion / delay / disruption of service, are problematic.

Lately, Army G-6 is nuancing the “no blogs on the NIPRNET” policy, saying in meetings and email and other venues something different than what’s in the ARs and what they’re stating to people in their “you’ve violated Web policy” review notifications. For instance, an email from the Army G-6’s Policy Division said: “We have no issues with any [blogs] on a controlled-access .mil Website [i.e., AKO]. The issue is that they should not be on a public Website **unless the information is cleared by a public official before posting.**”⁴⁴⁵ That seems to leave the door open for blogging on the Internet if the blog is cleared beforehand – we’ll discuss the clearance process in a bit.

So we come to **brick wall #4, “we can’t do this on the NIPRNET, but we can’t be off the dot-mil domain?”** As we said, AR 25-1 and AR 25-2 drive usage of the Internet toward [army.mil](#). For example, the domain policy:

- Paragraph 6-7b(1), AR 25-1: “Per DoDI 8410.01, organizations must use the ‘[army.mil](#)’ domain as their second-level domain name for the [NIPRNET] and ‘[army.smil.mil](#)’ for the [SIPRNET], unless a **waiver** has been granted by the CIO/G-6 and, in turn, the DoD CIO. Requests for a waiver must explain the rationale for the use of any domain other than [army.mil](#) on a temporary or permanent basis.”
- Paragraph 6-7a(2) and (5), AR 25-1: “Any organization desiring Web capabilities that would duplicate services already available on AKO / DKO must request a **waiver** from the CIO / G-6. See also Paragraph

“Telling the Army story goes beyond generating press releases and responding to media queries. We must use the full array of communications in the dynamic information environment in which we live – and in which our Army families live and our Soldiers fight. That includes public events, Internet, blogs, as well as traditional TV, radio and newspapers. Strategic communications is more than what we say or how we say it – it is actions and images that tell a story and match our words.” – Secretary of the Army Pete Geren, “Warrior Transition Units Media Coverage and the Upcoming Communications Effort on Army Family Covenant” memo, May 21, 2008

⁴⁴⁴ This kind of hair-splitting was evident in the Aug. 3, 2009, Marine Corps-wide ban for a year to social-media site access and use from the Marine Corps’ enterprise network. (See <http://www.marines.mil/news/messages/Pages/MARADMIN0458-09.aspx> for text of the order.) Blogging on AKO is done via an “SNS-like service,” to use the Marines’ phrase, whereas blogging on a commercial site is just plain ol’ blogging.

⁴⁴⁵ Email forwarded to TRADOC March 12, 2009. Original from Army CIO G-6 Policy Division to OCPA OSMD.

6-7b for policy concerning use of .mil domains, required waivers, and exceptions.” Paragraph 6-7b(2) details the exceptions to this policy that do not require waivers. TRADOC-related exceptions include 1) Army Reserve-officer training units that do not fund or operate Internet systems, but instead use the domains of their hosting organizations or the organizations that support their Internet communication needs; and 2) Army recruiting Websites in the public domain, which may be hosted and served in a commercial Web domain. Paragraph 6-7b(3) details examples of special needs or requirements that may be approved for domains other than [army.mil](#). Paragraphs 6-7(4) and (5) give instructions for waiver requests, including all items that must be included in the justification.

- Paragraph 6-7a(6), AR 25-1: “ACOMs, ... service schools or centers, installations, division-level units, and special-service organizations will establish third-tier level Websites and will consolidate subordinate organizations into these sites ... to **minimize the total number of Army Websites**. All other organizations may have a Web presence (for example, Webpages) on the Websites of their respective parent organizations.”

And the ISP policy:

- Paragraph 6-4o, AR 25-1: “The only authorized access from Army computers, systems, and networks to the Internet is through a [Defense Information Systems Network (DISN)]-controlled and -monitored connection. **Exceptional situations** may exist where Army organizations connected to the NIPRNET may also require direct connection to the Internet, for example, through an [ISP].”
- Paragraph 4-20g(3) and (6), AR 25-2: “Government-owned or leased ISs will not use commercial ISPs ... as service providers, **unless a government-acquired subscription to such services is in place and the access is for official business or meets the criteria for authorized personal use** as indicated in AR 25-1, Paragraph 6-1. Commercial ISP services are authorized to support ... organizations identified in paragraph 4-20b(2), ... and no cross or direct connectivity to the NIPRNET will exist or be implemented.”
- Paragraph 4-20b(2), AR 25-2: “Proponents for programs that require network services for family members, retirees, and other individuals serviced at Army installations ... should arrange for services through a commercial [ISP] or other isolated connection capability. ... These connections are unofficial communications and will be isolated either logically or physically from official DoD and Army NIPRNET networks.” According to Paragraph 4-22d, AR 25-2, isolation includes “physical isolation (unplugging the network connection), restricting any direct physical access, and logical isolation (blocking the IP at security routers or firewalls both inbound and outbound) from the network to the system.”
- Paragraph 4-20c(2), (3) and (4), AR 25-2: Supervisors and managers will authorize commercial ISP accounts per Chapter 6, AR 25-1; ensure there are no cross-connections directly between the Internet and NIPRNET of ISs; and permit direct connections to the Internet to support electronic commerce when those systems will not connect to the NIPRNET or the SIPRNET.

So **ISPs are possible if a waiver is requested and the computer uploading to the ISP is isolated from the NIPRNET**. This has been a hard case to plead so far, but at the 2009 Army Worldwide Public Affairs Symposium, Mike Krieger, deputy Army CIO / G-6, and Maj. Gen. Kevin Bergner, Army CPA, agreed publicly at the close of Krieger’s presentation that a commercial line was a permissible option for Public Affairs personnel.

Since G-6 is responsible for protecting the Army’s networks, any option that offers protection is more agreeable to those professionals, but another community whose clearance / review is required for anything going out into the public domain (see Chapter 3) is less enchanted with this option. Thus, **brick wall #5, the clearance process, especially the OPSEC review**.

Soldier and DA civilian blogging done from home computers, or even on government-owned computers in deployed areas, comes under the umbrella of **unofficial blogging**. PAO and / or commander / leader blogging is **official blogging**. There is a **difference in the clearance process**.

In general, policy governing blogs is included in AR 530-1, especially Paragraphs 2-1g(1), 2-2c, 2-21c, and E-3; ALDODACT 11/06; DoDD 5230.9; and DoDI 5230.29. We also recommend ALARACT 156/2005.

Unofficial blogging and other uses of social media. There are several characteristics of unofficial blogs that differentiate them from official blogs. Unofficial Internet blogs are 1) the personal thoughts, ideas, knowledge, experience, and opinions developed and disseminated by a Soldier or DA civilian employee 2) in an off-duty status (on personal time) and 3) not as part of his / her official duties, posted to 4) Soldier- or DA civilian-owned and -

maintained sites (not funded with DoD funds). 5) These unofficial Websites or blogs are located on commercial networks (e.g., .com, .org, .biz, .edu). ALDODACT 11/06, published Aug. 9, 2006, defines the personal blog as one not having DoD sponsorship and purpose; it further states that personal blogs may not be created on duty time and may not contain information on military activities not available to general public.

DoD recognizes that service members are its best spokespersons. It encourages positive efforts and Soldiers' pride in their jobs. Caution, however, is appropriate because the military is on a war footing, and we have an enemy who not only appreciates our shooting ourselves in the foot with what we release to the world, but is able to pick that bullet up and shoot us with it again.

This, however, does not imply "censorship" of Soldiers' personal blogs. A few years ago, the revised / reissued AR

"The free flow and sharing of information is diametrically opposed to some of the security things people are obligated to protect. If the intelligence community can [use Internet tools such as Intellipedia, its version of the on-line encyclopedia Wikipedia], the rest of government probably can, too." – Maxine Teller, DoD's new-media strategist, quoted in "Agencies test new waters in social media" by Elizabeth Newell, govexec.com, Feb. 19, 2009

530-1 raised furor in the media via several "the Army is playing Big Brother / denying Soldiers their First Amendment rights / holding something back from the public" stories. Although AR 530-1 was previous policy, just reissued, the public discussion was so hyperbolic that the Army issued a fact sheet May 2, 2007, entitled "Army Operations Security: Soldier Blogging Unchanged." As stated in the fact sheet, "America's Army respects every Soldier's First Amendment rights while also adhering to [OPSEC] considerations to ensure their safety on the battlefield. In no way will *every* blog post / update a Soldier makes on his / her blog need to be monitored or first approved by an immediate supervisor and [OPSEC] officer. **After receiving guidance and awareness training from the appointed OPSEC officer, that Soldier blogger is entrusted to practice OPSEC when posting in a public forum.**"

The fact sheet says that Soldiers may have a blog without needing to consult their immediate supervisor and OPSEC officer if the blog's topic is not military-related (i.e., Sgt. Doe publishes a blog about his favorite basketball team); the Soldier doesn't represent or act on behalf of the Army in any way; and the Soldier doesn't use

government equipment when on his /her personal blog. But the fact sheet says that a Soldier should inform his or her OPSEC officer and immediate supervisor anyway when establishing a blog for two reasons: to provide the command situational awareness; and to allow the OPSEC officer an opportunity to explain to the Soldier matters to be aware of when posting military-related content in a public, global forum.

The overarching DoD policy on releasing public information, DoDD 5230.09, Paragraph 4g, states: "DoD personnel, while acting in a private capacity and not in connection with their official duties, have the right to prepare information for public release through non-DoD fora or media. This information must be reviewed for clearance if it meets the criteria in DoDI 5230.29. ... Such activity must comply with ethical standards in [DoDD 5500.07 and DoD 5500.7-R] and may not have an adverse effect on duty performance or the authorized functions of [DoD]."⁴⁴⁶

Therefore **unofficial blogs do not have to be cleared** (the blogger just has to be trained in advance by the OPSEC officer) **unless the content meets the criteria in DoDI 5230.29 for national-security information**; then it must be cleared IAW procedures outlined in the DoDI.

Policy in AR 360-1 is generally applicable to social-media content:

- Paragraph 6-6c, AR 360-1: "Unofficial materials do not require clearance. These include materials produced on personal time, using personal equipment and open sources. ... It is the author's responsibility to ensure security is not compromised."
- Paragraph 5-13, AR 360-1: "Army personnel may express personal opinions unless limited by law or regulation. They should discuss candidly matters about which they have personal knowledge if the information is not classified or otherwise non-releasable. When questioned on a classified matter, they will state frankly that the information cannot be discussed."

⁴⁴⁶ Also stated in Paragraph 6-8, AR 360-1.

Official blogging and other social-media use. An official blog, on the other hand, is the inverse of an unofficial blog: it may be the personal thoughts or ideas of someone, but an official blog meets one of these conditions:

- The blogging is done on duty time (not personal time);
- The blogging is done as part of the blogger's official duties;
- The blog is initiated by a specific Army organization;
- The blog contains content where the blogger identifies himself / herself as a member of the Army.⁴⁴⁷
- The blog is typically paid for via DoD funds.

When individuals post official information, these **blogs must be reviewed and cleared by appropriate security experts and PAOs prior to release**. In fact, the DoD policy requiring clearance, by appropriate security review and PAOs prior to release, of "any official information intended for public release that pertains to military matters, national-security issues, or subjects of significant concern to the DoD" is inclusive of "materials placed on the Internet or released via **similar electronic media**" – in other words, social media.⁴⁴⁸

As stated in the "unofficial blogging" section, the policy *does not apply* to personnel posting in a private capacity (i.e., not identifying themselves as connected to an Army component) on subjects not involving Army business or issues. Examples of non-application include maintenance of private Website content on matters unconnected to the Army such as hobbies, sports, or religion, or posting to a blog as a private citizen.

The differentiation in the clearance policy is because official blogging is "publishing" – in other words, the public release of information in an official capacity – and therefore is subject to the laws, rules, and regulations that govern the public release of information, including DoDD 5230.9, DoDI 5230.29, and ALDODACT 11/06, which require OPSEC and security review for all information released into the public domain.

Official writing and public-speech guidelines also apply:

- Remarks must address a subject within a speaker's official expertise. This policy does not prevent DA military or civilian members from speaking on matters unrelated to the official concerns of the U.S. government when such activities are consistent with other laws and regulations and do not conflict with official duties or imply government endorsement.⁴⁴⁹
- Official writings must not contradict U.S. government policy or law. They must adhere to DoD 5500.7-R.⁴⁵⁰
- In general, Army employees will not officially endorse, or appear to endorse, membership drives or fund-raisers for any non-federal entity. (See DoD 5500.7-R.)⁴⁵¹
- Situations where an event's real or apparent purpose is to stage controversy and / or confrontation will be avoided.⁴⁵²

"The whole goal is to get information out where the people are going. They're going to YouTube, not government video sites. They're going to Facebook, so we're trying to get there. We need to syndicate government content so we can put it where people already are. The public should be able to choose what channel they use." – Bev Godwin, director of USA.gov and Web best practices at GSA's Federal Citizen Information Center, quoted in "Agencies test new waters in social media" by Elizabeth Newell, govexec.com, Feb. 19, 2009

⁴⁴⁷ If the blogger states or implies Army affiliation but wishes to blog in an unofficial status, he / she should use this disclaimer adapted from Paragraph 6-8c(2), AR 360-1: "The views expressed in this blog are those of the blogger and his / her guests and commenters, and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. government."

⁴⁴⁸ Paragraph 5-1, AR 360-1.

⁴⁴⁹ Paragraph 6-7a, AR 360-1.

⁴⁵⁰ Paragraph 6-7e, AR 360-1.

⁴⁵¹ Paragraph 6-7f, AR 360-1.

⁴⁵² Paragraph 6-7h, AR 360-1.

- Material must not endorse, promote, or sponsor any private individual, group or venture, or give the appearance of doing so. The event itself should be of common public interest and benefit.⁴⁵³
- Any individual who uses a title or other identification connected with DoD in an unofficial writing will include with his / her material a disclaimer IAW Paragraph 6-8c(2), AR 360-1. (See Footnote 447.) The writer will not use a title or other DoD identification in connection with the material if requested to refrain from doing so by the reviewing authority.⁴⁵⁴
- No Army personnel – including ARNG and USAR forces – acting in their official capacity, may engage in public commentary concerning political campaigns or elections without prior clearance from the office of the ASD-PA.⁴⁵⁵
- Official blogging should have a purpose, not merely be for self-aggrandizement, and be of value to the general public.

The one item of policy that seems to run counter to local “empowerment” of official blogging is the DoD policy memorandum for IIA, dated June 8, 2007. To legitimately exist, according to this memo, there is an additional benchmark: MILDEP blogs must address manpower issues within the organization or address organizing, training, and equipping their departments. And, ASD-PA is the approval authority for Public Affairs’ activities IIA. This authority cannot be delegated from the ASD-PA, according to the memo. Yet ASD-PA has not provided guidance to the MILDEPs vis-à-vis procedures for gaining its approval. The memo does not specify whether ASD-PA must grant permission to anyone within the MILDEPs to establish and maintain a blog; some have said that ASD-PA does view this as its authority. Many, including experts at DoD Public Affairs, see this memo as only applicable to IIA whose audiences are foreign.

Whether given permission by ASD-PA or not, the Army’s official use of social media can be likened to a horse race where the horses are well out of the gate. There are several official blogs, Facebook pages, and Twitterers, for instance:

- The Army’s official blog is <http://armylive.dodlive.mil>. The blog provides a top-level approach on Army issues, as well as news and updates on activities and events taking place in the Army and OCPA. TRADOC’s official blog is <http://tradoclive.dodlive.mil/> – like Army’s official blog, TRADOC has been given “permission” by ASD-PA (dodlive.mil is DoD Public Affairs’ official blog site).
- A unit-sponsored blog, www.hammerpao.com, is written by a team of PAOs. This blog provides localized information and news stories, but adds the dimension of comments and conversation.
- A commander-written blog usually takes speeches or official statements and crafts them into a post. Maj. Gen. Michael Oates, 10th Mountain Division commander, however, writes a blog (<http://www.taskforcemountain.com/mountain-soundoff>) that’s more like a Web forum, sparking comments and conversation from his Soldiers.
- Maj. Gen. Elder Granger’s blog (<http://www.health.mil/tmablog>) during his time as TRICARE deputy director included a mixture of posts from him as well as articles, information, and updates from other staff members.
- Along with the Army’s official Facebook page, Gen. Ray Odierno, Multi-National Force-Iraq commander, has a Facebook fan page. It includes information about official events, travel, and milestones taking place across Iraq.
- You may follow TRADOC’s Facebook fan page at <http://www.facebook.com/USArmyTRADOC>.
- 1st Brigade, 1st Armored Division’s Facebook page links to articles about the unit and provides updates useful to family, friends, and supporters.
- Lt. Gen. Rick Lynch, commanding general of III Corps and Fort Hood, Texas, has a Facebook page populated with news and information generated from official speeches and public statements.
- Navy Adm. Mike Mullen, chairman of the Joint Chiefs of Staff, is on Twitter at www.twitter.com/thejointstaff. He posts links to news items of interest or provides his thoughts on a particular topic.

⁴⁵³ Paragraph 6-7i, AR 360-1.

⁴⁵⁴ Paragraph 6-8d, AR 360-1.

⁴⁵⁵ Paragraph 3-4a, AR 360-1.

- The Army's official Twitter link is <http://www.twitter.com/USArmy>. TRADOC's is <http://twitter.com/tradoc>.
- 4th Battalion, 3rd Infantry Division, uses Twitter to communicate between commanders and Soldiers. Messages include "praise tweets" or performance "chastisements." Because most individuals using Twitter connect it to their mobile devices, it's a good way for commanders and leaders to connect with their Soldiers while on the go.
- The Army has several other official sites on commercial social media: Flickr (for photo sharing), <http://www.flickr.com/soldiersmediacenter>; YouTube (for video sharing), <http://www.youtube.com/soldiersmediacenter>; Vimeo (for video sharing), <http://www.vimeo.com/usarmy>; and Delicious (for integrated bookmarking), <http://delicious.com/USArmyMedia>. TRADOC is also on Flickr (<http://www.flickr.com/photos/37859509@N02/>), Wikipedia (http://en.wikipedia.org/wiki/United_States_Army_Training_and_Doctrine_Command#TRADOC_Priorities), Delicious (<http://delicious.com/tradoc>), and Vimeo (<http://www.vimeo.com/tradoc>).

The clearance process brings up **brick wall #6, social media violates OPSEC**. Sometimes it might, just like another other public venue could have OPSEC violations if personnel aren't well-trained enough. One, our young Soldiers are digital natives and expect free, unhindered communication. Since the private and public domains merge in their minds (for instance, studies show that they have a false sense of privacy – when sharing information on SNS, they think the info stays with "friends"), the potential solution is to encourage, educate, empower, and equip them.⁴⁵⁶ No one controls all aspects of OPSEC – the countermeasure is to give social-media users OPSEC training specific to Web and social-media content (see Chapter 6 for the Army's mandatory training) and to accept risk because the "good" of using social media outweighs the "bad."

It's a matter of common sense as well as a sense of accountability and responsibility. As an upcoming OCPA publication states: "[I]t is important for Soldiers as well as Public Affairs professionals to remember the two guiding

"As we're building government space on-line, there are still some issues. We can't sign away indemnity, nor can we say that if there's an issue California law will prevail, because if a federal agency is involved, it's always federal law." – Bev Godwin, director of USA.gov and Web best practices at the General Service Administration's Federal Citizen Information Center, quoted in the article "Agencies test new waters in social media" by Elizabeth Newell, govexec.com, Feb. 19, 2009

documents that apply to all public communication: [OPSEC] and the [UCMJ]. ... Soldiers must maintain professional conduct and good order and discipline in the virtual world in the same ways they would in the real world. Special care should be taken to ensure that public-facing profiles, to include Facebook pages and sites, present an appropriate picture of Army life. ... Social media is all about taking your identity or messaging and turning over control to your community. A Facebook wall and a Flickr comments stream are places for both positive comments as well as negative ones. If you're not willing to lose control of the message and give some of the power to your community, social media is not for you."⁴⁵⁷

Brick wall #7 is social-media sites' user agreements. Current user agreements and terms of service imply inherent legal liabilities that DoD can't incur, but a **federal-wide waiver is being worked**. YouTube, Facebook, and Twitter, for instance, require users to sign an agreement that allows advertising and establishes legal jurisdiction / indemnity, among other things, while government users operate under federal rules and policies.

Expected future policy and best practices. We've been putting the cart before the horse a bit in this section about what's coming

in the future, but we can be sure there will be change. Government-wide guidance on how agencies can more fully use social media is forthcoming, according to Vivek Kundra, the federal CIO and OMB's e-government and IT administrator.⁴⁵⁸ Kundra has said that the Federal CIO Council and GSA are working on the "rules," and that GSA signed agreements with four video-sharing and social networks recently to provide services that comply with federal

⁴⁵⁶ From "New Media and the Warfighter" presentation by Professor Dennis Murphy, Army War College.

⁴⁵⁷ From draft TTP on social-media best practices, being prepared by OCPA's OSMD.

⁴⁵⁸ From "Government working on rules for Web social networks," reported on NextGov.com, April 28, 2009.

terms and conditions. (Brick wall #7 is softening.) Kundra said it could take time to align the new policy with statutes like the Presidential Records Act and Privacy Act, both enacted in the 1970s, and the 7-year-old FISMA.

The DEPSECDEF recently issued a memo⁴⁵⁹ directing DoD CIO / G-6 to present to the SECDEF's attention no later than Aug. 31 a report on the threats and benefits, as well as policies and processes, of Web 2.0 capabilities and SNS. The DoD CIO is also tasked to develop DoD policy governing the use of Web 2.0 capabilities "from a comprehensive risk management perspective" no later than Sept. 30. The risk-management approach gives us pause, but we'll know soon where DoD's top brass stand.

OCPA is also working on updated policy, including revisions to AR 360-1 that include unofficial Web publishing and blog guidance, plus TTPs on official use of social media. The draft AR 360-1 gives Soldier bloggers their parameters and trusts them to make responsible decisions, as previous guidance has done. Before the DEPSECDEF's memo came out, the Army CIO / G-6 was also working on updated policy for social-media use. It's possible that a command policy letter signed by CG TRADOC, however, will be published before any Army-level policy or best practices are published.

AR 360-1's expected additions will guide Soldier and DA civilians in personal use of blogs on commercial networks (e.g., .com, .org, .biz, .edu). Like the May 2007 blogging fact sheet, bloggers will be expected to support individual freedom of speech and expression, but at the same time demonstrate good order and discipline, reflect the Army Values, and safeguard the privacy and safety of fellow Soldiers by not making available their PII or the OPSEC of their military units or missions. We expect the following to be some of the key parameters:

- Personal Websites and blogs produced in a personal capacity and not in connection or reference to official duties do not require advance clearance.
- It is the personal responsibility of Soldiers, DA civilians, and DoD contractors to ensure that any personal Websites and blogs do not contain unreleasable information. Commanders and other officials will be responsible for holding personnel accountable for adhering to the tenets of the OPSEC regulation (AR 530-1) and any other applicable policies addressing communications.
- Personnel must add a disclaimer to unofficial personal Websites in which the individual refers to him or herself as a Soldier, employee, or contractor of the U.S. Army to preclude readers from assuming unofficial sites represent an Army position.
- Reasonable restrictions on free speech such as "no political commentary while in uniform" extend to electronic communication.
- Government employees will be responsible for ensuring that information posted does not put themselves, other employees, or their families at risk.
- All visual information – still and video imagery – provided directly to any media outlet, organization, public Website, family, or friends, whether in hard copy or electronic form, will be subject to DoD and Army policy.

In addition to the social-media changes in AR 360-1, discussed as unofficial Web publishing, OCPA plans to publish social-media TTPs. (No date for publication has been given.) We expect some of the key elements of the Army's approach to social media to be:

Army leaders and communicators need to observe and understand what is being communicated on the Web and how it is being communicated. Posts on blogs and Websites provide indicators of communications challenges and needs relevant to our mission, policies, and people. If we do not, we abdicate our hard-earned credibility and positive relationship with key stakeholders and influencers to sensational-driven news and opinion media. Moreover, our Public Affairs programs will falter under the increasing pace of technological change, coupled with individual actions that can have immediate strategic implications.

Increasingly, individuals are looking to the Web as their primary source of news and information. As an Army, we have an obligation to tell our story in the spaces and places where our community is already engaging.

⁴⁵⁹ "Web 2.0 Capabilities and Social Networking Sites," July 31, 2009.

- The Public Affairs mission is to execute a comprehensive Public Affairs program that effectively integrates both traditional and IIA. It will be **mission-critical to dedicate full-time assets** to manage a program that includes both traditional media and IIA.
- Public Affairs will be expected to **monitor what is being discussed** about its sphere of influence, provide information to these discussions, and proactively seek new audiences to engage.
- PAOs will also be responsible for conducting **periodic reviews** of their organization's IIA – not less than semi-annually.

There are several interesting aspects of the draft CIO / G-6 policy (entitled “Use of Social Media Tools in the Army”):

- It recognizes that **official government sites may be established on commercial sites**. IAW Paragraph 6, official government sites on social-media outlines may not contain political or discriminatory content; may not endorse or appear to endorse or show favoritism to non-federal entities; must reflect U.S. government policy; and may not appear to endorse views contrary to U.S. government policy. Organizations authorized to establish official social-media sites must receive training on the scope and authorized uses of social-media sites, and ensure Public Affairs, privacy, and OPSEC review of content before release or disclosure.
- This policy reiterates that **Soldiers and civilians using social-media sites for unofficial purposes** (i.e., they hold personal accounts on social-media sites) **may not use these sites / their accounts on official duty time**. IAW Paragraph 7, “[p]ersonal accounts should not be established with government email addresses, employ the use of government logos, be used to conduct official business, release official agency information, or be used for any other official communication related to the employee's government job or activities. Agency personnel [using] social-media technologies must comply with the [JER] and the Standards of Ethical Conduct for Employees of the Executive Branch (see 5 CFR Part 2635). These rules include the prohibition of release of non-public information, require appropriate disclaimers of opinions being expressed, and restrict the use of government computers to access and manage personal sites during official duty time.”

TRADOC social-media policy is expected to address both unofficial and official use of social media. For instance, unofficial blogging is expected to be encouraged off the dot-mil domain as long as personnel are aware of pertinent regulations, while official bloggers are expected to be limited to command spokespersons. Public release of information in an official capacity via use of social media is expected to be subject to the laws, rules, and regulations that govern the public release of information, including the clearance process.

Social media as community relations. Unofficial posting on Internet discussions is considered congruent with the PAO core function of community relations because the postings are interpersonal, interactive communication. Guidance on Soldiers' participation in community relations can be found in Paragraph 8-1b(1), AR 360-1: “Programs that involve direct contact with the civilian community are the most effective unofficial means of improving community relations. Commanders should encourage military and civilian personnel and their family members to participate as private persons in local community activities such as educational, religious, organizational, recreational, and youth projects.”

Army presence in social-media outlets creates a known and trusted presence. People trust people they know, not institutions or officials. People may judge news received via trusted social networks to be more credible than news received via traditional media.

TRADOC PAO suggests that engagement in social media be considered a community activity – whether the social-media venue is educational, religious, organizational, recreational, a youth project, or other category, it doesn't matter. Social media can be an effective channel of two-way communication between the Army

and the community⁴⁶⁰ if used judiciously (although not quite the traditional communication between commander and community). If social-media engagement is successful, the community formed by the engagement could become a grassroots “community-relations council” – but a caveat: since it would be grassroots, there is no planning and

⁴⁶⁰ Paragraph 8-1c(1)(a), AR 360-1.

organizing it IAW Paragraph 8-1d, AR 360-1. As we've said previously, there is risk in social-media engagement; social-media engagement must be approached with thought and purpose, not as a bright, shiny, new toy to play with.

WEBPAGE DESIGN AND CONTENT FORMATTING

The elements of Webpage design and formatting as they affect content will be discussed in this section. The Army requires its Webmasters to ensure that their Website pages are designed, developed, and tested for multiple browsers, operating systems, connection speeds, and screen resolutions, based on an analysis of an organization's Website visitors. These requirements can affect the inclusion of content and will affect the look and feel of a Website – part of the Website coordinator / Web-content manager's concern.

Links. Since links are considered content, considerations for Website / Webpage designers follow.

Every Webpage written for TRADOC Websites should have links to logically previous Webpages or higher-level Webpages. For easier navigability, we recommend that links for the site's homepage be placed on each interior page. For Web-based documents such as reports that must flow in a page-by-page order, we recommend links to the site's homepage from at least the document's cover page and its table of contents, and to the document's next and previous page from each internal page. We recommend these logical "next" and "previous" links because the browser back button can be confusing if, for example, a user hyperlinks from Section 1 of a document to Section 3 and then wants to logically go "back" in the document to Section 2; clicking the browser's "back" button ordinarily takes him / her to Section 1. The bottom line is that the **text links or graphical links (buttons) should give predictable access from and to all pages.**

Organization Websites that link to documents requiring downloading should provide enough contextual information that visitors have a reasonable understanding of what to expect when they view the material after downloading it.

Proprietary formats. Proprietary formats should be used only when the audience is known to have easy access to software able to read the format. Since the capabilities of a publicly accessible Website's audience are so varied, documents using a proprietary format should be posted to the organization's AKO access-controlled portal. If the document must be posted to the publicly accessible Web, raw data files provide the greatest flexibility for the public and are preferred over proprietary formats requiring specific commercial software.

Organizations must not burden the public with a format that requires use of a plug-in, applet, or other application to interpret page content unless the following conditions are met:⁴⁶¹

- The page provides a text link (no icons) to the plug-in or applet.
- The organization has considered the intended use of the material by the target audience.
- The plug-in, applet, or other device is accessible to the target audience.
- The level of effort required to convert the material is minimal.

As listed in the first condition, when a Webpage requires an applet, plug-in, or other application to interpret page content, the page should provide a text link to a plug-in or applet.⁴⁶²

Horizontal rules. Don't abuse horizontal rules (<hr>) tags. We recommend that you use them one at a time, and only to logically divide unrelated sections of a single page. In most cases, a simple paragraph break (<P>) is preferable.

Navigation. Websites not required to use the TRADOC corporate template must use consistent navigation between and within their pages. Website visitors are more likely to gather the information they're looking for if changing

"Agencies should be required and funded to do user testing before undertaking major improvements to any current Website, or launching a new Website. Agencies should use their Website to publish a summary of common customer comments and explain the actions they are taking in response to the feedback. Doing so will create better transparency and accountability." – **Putting Citizens First: Transforming On-line Government**, Federal Web Managers Council whitepaper

⁴⁶¹ Paragraph 8-3b(4), DA PAM 25-1-1.

⁴⁶² Paragraph 8-3b(4), DA PAM 25-1-1.

navigation doesn't confuse them. Some required navigation will be outlined in the "required content" section later in this chapter – following are other standard navigation criteria.⁴⁶³

Common items appearing on most Webpages should be in the same location on each page and have the same appearance and wording. A navigation item that is shared by a group of pages (such as a set of pages on a single topic, or for a division of the organization) should also have the same location, appearance, and wording on each page.

Navigation items of the same type should look and behave like each other. For example, if a set of pages on one topic has subtopic links in the left navigation bar, pages on other topics should have subtopic links in the left navigation bar that are similar.

If a set of Webpages requires specialized navigation, that navigation is applied to the largest possible local grouping (such as a topic, an audience, or a complete organizational unit). The specialized navigation should be similar in appearance and behavior to the overall navigation scheme.

Color. Avoid the use of white type. No matter what background you use, the text will not show up on a printed copy of your page.

"Under construction." The Army discourages posting of "under construction" pages on its Websites. All Webpages are always technically under construction, but if one isn't ready for public viewing, Webmasters should not post it until it is final.

POLICY: CONTENT LIMITATIONS

In addition to the limitations on content discussed in Chapter 3, this section and the next one set forth other content standards for Website coordinators / Web-content managers.

Content and services provided via Army public Websites should not be redundant or in conflict with each other.⁴⁶⁴ To avoid redundancy or conflict, organizations should follow the policy of Paragraph 8-5b, DA PAM 25-1-1.

To increase information value, Webmasters should organize content on Websites / Webpages and portals by subject / topic, by audience group, by geographic location, or by any combination of these factors, based on an analysis of the visitor's needs. Content should be the main focus for the target audience and serve as a general index to all major options available on the Website. Homepages should minimize extraneous content to allow visitors to get to the content they need and want most.⁴⁶⁵ How a Website or portal should **not** be organized is by organization chart.

External links. Although external links and the content found at those links are not a federal QI standard,⁴⁶⁶ they are discussed as a Web-quality standard in the DoD Web policy. Therefore TRADOC PAO recommends that external links be considered as a TRADOC QI standard. The requirements on links are specified following and in a later section of this *Guide* labeled "required links."

The external-link standards are:

- Hyperlinks to Web resources other than official U.S. government Web resources are permitted only if the organization's mission requires them. Organizations must review links to content on other organizational Websites or to portals and specialized Websites regularly to ensure links are current and accurate, and that they have continued suitability.⁴⁶⁷
- Organizations must establish objective and supportable criteria or guidelines for their selection and maintenance of links to external Webpages.⁴⁶⁸
- External links may have no product endorsements or preferential treatment.⁴⁶⁹
- No compensation of any kind may be accepted in exchange for a link placed on an organization's publicly accessible official Army Website.⁴⁷⁰

⁴⁶³ Paragraph 8-3b(7), DA PAM 25-1-1.

⁴⁶⁴ Paragraph 8-5a, DA PAM 25-1-1.

⁴⁶⁵ Paragraphs 8-2c and 8-2d, DA PAM 25-1-1.

⁴⁶⁶ Paragraph 3D, Attachment, OMB memorandum M-05-04, "Policies for Federal Agency Public Websites," Dec. 17, 2004.

⁴⁶⁷ Paragraph 7.1.1, Part II, DoD Web policy; Paragraphs 8-1k(3) and 8-5b(6), DA PAM 25-1-1; Paragraph 5-5b(4), TR 25-1.

⁴⁶⁸ Paragraph 7.1, Part II, DoD Web policy; Paragraph 6-7c(7), AR 25-1.

⁴⁶⁹ Paragraph 7.1.2, Part II, DoD Web policy; Paragraph 5-5b(4), TR 25-1.

- External links may not require or encourage users to choose any browser-specific software.⁴⁷¹
- An external link uses only text or hyperlinked text to direct visitors to non-Army software download sites;⁴⁷² there are no company graphics or logos permitted as graphical links, as this is considered endorsement. (This includes the icons for social-media sites.) If the organization uses graphical links in other circumstances, it must also use text links to comply with Section 508 law.
- If an organization is using frames to link to external sites, the organization will consult legal counsel concerning trademark and copyright issues.⁴⁷³
- If an organization links to an MWR or to another authorized site that contains commercial advertisements or sponsorships, a disclaimer must be given IAW Paragraph 7.2, Part II, of the DoD Web policy.⁴⁷⁴ The organization must also use the non-endorsement disclaimer if linking to a non-government Website (this includes to contractors who produce DoD Websites) that “neither the DoD nor the organization endorses the product or organization at the destination, nor does the DoD exercise any responsibility over the content at the destination.”⁴⁷⁵ The Army’s standard for the disclaimer is that it must appear on the page(s) listing the external link or through an intermediate “exit notice” page generated by the server. The Army’s standard applies to links for any site other than an official DoD Website.⁴⁷⁶ See Paragraph 7.2, Part II, of the DoD Web policy; Paragraph 6-7c(7)c, AR 25-1; or Appendix D of this **Guide** for the exact external-links disclaimer text.
- If a link is made to one non-DoD site, the organization must link to all similar sites if requested.⁴⁷⁷
- No .mil Website may be directly linked to or refer to Websites created or operated by a political campaign or committee.⁴⁷⁸
- When an organization’s Website provides information or services for which there is a corresponding government-wide portal or specialized site, the organization should link to the government-wide portal or site from its pages on that topic. (For example, Warrior Ethos discussed in training stories could link to an Army Warrior Ethos Web microsite on www.army.mil.) Conversely, when a government-wide portal or specialized Website is available on a subject that the public would expect to find on an organization’s site (i.e., Warrior Ethos, since it is a foundational concept in Soldier training), but the organization does not provide that information, the organization should link to the government-wide portal or site in a logical and useful location.⁴⁷⁹
- Organizations must not link to government-wide portals or specialized information unless they are related to the organization’s mission or function, or might be seen as being related. Links that are not related to a Website’s content can be deceptive and confusing.⁴⁸⁰
- Organizations may not re-post documents that other organizations originate. Instead, they must provide links to those documents posted on the Websites of the content owners – considered the original, authoritative source. Organizations should consult with each other to find ways to share or coordinate content and to mitigate duplication.⁴⁸¹
- If organizations use external links, they must also post a link to an explanation of their “process for linking to non-Army sites,” which will include guidelines for selecting and maintaining external links. Organizations’ linking procedures must explain why some links are chosen and others are not. The links must be chosen fairly and in the best interest of the public.⁴⁸² The linking policy found at USAGov.gov is

⁴⁷⁰ Paragraph 7.1.3, Part II, DoD Web policy; Paragraph 6-7c(7)a, AR 25-1.

⁴⁷¹ Paragraph 7.1.4, Part II, DoD Web policy.

⁴⁷² Paragraph 7.1.4, Part II, DoD Web policy; Paragraph 8-1k(1), DA PAM 25-1-1.

⁴⁷³ Paragraph 7.1.5, Part II, DoD Web policy.

⁴⁷⁴ Paragraph 7.1.6, Part II, DoD Web policy.

⁴⁷⁵ Paragraph 7.1.7, Part II, DoD Web policy.

⁴⁷⁶ Paragraph 7.2, Part II, DoD Web policy; Paragraph 6-7c(7)c, AR 25-1.

⁴⁷⁷ Paragraph 7.1.8, Part II, DoD Web policy.

⁴⁷⁸ Paragraph 8-2b(2), DA PAM 25-1-1.

⁴⁷⁹ Paragraph 8-5b(2) and 8-5b(3), DA PAM 25-1-1.

⁴⁸⁰ Paragraph 8-5b(4), DA PAM 25-1-1.

⁴⁸¹ Paragraph 2.3, Part II, DoD Web policy; Paragraph 8-5b(1) and Paragraph 8-5b(5), DA PAM 25-1-1.

⁴⁸² Paragraph 8-1k, DA PAM 25-1-1.

recommended as an example for developing Army public Website-linking policies. TRADOC entities are encouraged to adopt the template in Appendix L.

- Listings of Web links on Army Webpages must separate external Web links from government and military links.⁴⁸³

Content duplication. Closely related to the considerations governing external links are the standards regarding content duplication. Because these requirements are also contained in the DoD Web policy, they are viewed as quality standards for the TRADOC publicly accessible WWW. The overarching standard for TRADOC is: **No TRADOC organization may duplicate on its Website or portal information that is available on another Army, DoD, or other federal-government Website.** Specifications on, and exceptions to, this standard are outlined following.

Before creating new information, the organization first determines if that same or similar information already exists within its organizational Website or on another Army, DoD, or federal Website⁴⁸⁴; to prevent duplication on the WWW, an organization must limit its Website content to only information for which it is responsible and must link to existing government-wide portal or specialized sites rather than recreating these resources themselves.⁴⁸⁵ (The standards for external links would then apply.) In the event of duplication on others' sites, links will be to the original, authoritative source.⁴⁸⁶

Organizations may mirror / replicate information if there are compelling performance, security, or other mission-related reasons,⁴⁸⁷ but this must be justified in writing as part of the pre-dissemination content-review process outlined in this *Guide*. The information provider must contact the owner of the original content and obtain written permission to replicate the information,⁴⁸⁸ and a copy of this written permission must be included in the request for content review as part of obtaining clearance to post information on TRADOC Websites.

No copyrighted information may be posted without the express written permission of the copyright owner.⁴⁸⁹ Organizations wishing to post copyrighted information must consult legal counsel and must provide a copy of legal counsel's opinion as part of the TRADOC content-review process.

Organizations must also establish a procedure with the original content owner for updating any information and for periodically verifying its releasability, currency, and accuracy.⁴⁹⁰

As the Army Publishing Directorate (APD) manages the only two authorized, official Websites for Army-wide administrative publications and forms, TRADOC organizations should not post duplicate copies of Army regulations or other Army-wide publications on their public Websites. Instead, if they desire to provide Internet access to departmental publications and forms on a Website, they should establish hyperlinks to the approved official publications and forms as listed in the official repository.⁴⁹¹ This not only saves server storage space and bandwidth, but it also helps ensure that the latest versions of the publications are accessible and not confused with older versions.

Portal administrators who manage controlled-access KCs for collaboration may wish to post publications for their collaborators' convenience – such private Websites are outside the scope of this *Guide*, but we encourage portal administrators to monitor APD on-line to obtain the most recent versions of documents.

POLICY: REQUIRED CONTENT

The policies and guidance also require certain types of content, including links, outlined in this section.

Required statements.

⁴⁸³ Paragraph 6-7c(7)b, AR 25-1.

⁴⁸⁴ Paragraph 8-5b, DA PAM 25-1-1.

⁴⁸⁵ Paragraph 2.3, Part II, DoD Web policy; Paragraph 8-5b(5), DA PAM 25-1-1.

⁴⁸⁶ Paragraph 5-3a(4)(b), TR 25-1.

⁴⁸⁷ Paragraph 2.3, Part II, DoD Web policy.

⁴⁸⁸ Ibid.

⁴⁸⁹ Ibid.

⁴⁹⁰ Paragraph 2.3, Part II, DoD Web policy.

⁴⁹¹ Paragraph 9-2b, AR 25-1.

Statement of organization's mission and outline of its structure. TRADOC organizations must include from their homepages a description (or link to the description from the homepage) of the organization's mission and the organization's structure (excluding names of personnel).⁴⁹²

Webmaster / portal administrator contact information. At a minimum, this must include the mission Webmaster's / portal administrator's generic email address for users to request information or direct questions, comments, suggestions, etc., for that organization.⁴⁹³

Currency declaration. The Army requires that each Webpage be clearly dated to show the date the content was posted or updated, and therefore requires a "currency declaration" on every Webpage to indicate to page visitors that the content is current and reliable. Each page must include a statement such as "Last updated on ____" or a "date stamp" on each page to indicate when last altered or reviewed.⁴⁹⁴ As proper customer / user service, the author of / POC for a publicly accessible Webpage can provide generic-email-address contact information or a generic "mailto:" link (such as monr.webmaster@monroe.army.mil) to Website visitors to contact if they find content to be incorrect, outdated, etc.

Sponsor. Each Webpage must state the organization's official name and display the phrase "This is an official U.S. Army site." Homepages and second-tier pages also include the organization's name identified as the site sponsor as part of the page title.⁴⁹⁵

Classification banner. Unclassified Webpages must be "marked" as to their classification, IAW AR 380-5. Each organization's unclassified Website homepage should include a banner stating that the Website contains only unclassified, non-sensitive, and non-Privacy Act information – Army policy requires this as the first page visitors come to. Although AR 380-5 states that a banner similar to the one given in Figure E-1 in that regulation will be used and that no further markings are required,⁴⁹⁶ AR 380-5 is ambiguous enough (and dated enough) that a better practice is for **personnel to use the banner given in AR 25-2 and the DoD Web policy when their Websites (or a portion of their Websites) / Web-based systems require authentication / logon**, such as restricted access areas linked from public Websites.

According to Paragraph 4-5m(6) and (7), AR 25-2, AR 25-2's access warning banner replaces the warning banner in AR 380-5⁴⁹⁷ and may not be modified further. This banner's wording is:

"YOU ARE ACCESSING A U.S. GOVERNMENT (USG) INFORMATION SYSTEM (IS) THAT IS PROVIDED FOR USG-AUTHORIZED USE ONLY. By using this IS (which includes any device attached to this IS), you consent to the following conditions: The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. This IS includes

⁴⁹² Paragraph 5-5b(2), TR 25-1.

⁴⁹³ Paragraph 5-5b(3), TR 25-1.

⁴⁹⁴ Paragraph 8-11, DA PAM 25-1-1.

⁴⁹⁵ Paragraph 8-1i, DA PAM 25-1-1; Paragraph 5-5b(5), TR 25-1.

⁴⁹⁶ Paragraph E-6, AR 380-5. The banner in AR 380-5 reads: "WARNING! UNCLASSIFIED, NON-SENSITIVE, NON-PRIVACY ACT USE ONLY. This is a Department of Defense (DoD) interest computer system. This system is monitored to ensure proper operation to verify the functioning of applicable security features and for other like purposes. Anyone using this system or any other DoD computer system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials. Unauthorized attempts to upload or change information, to defeat or circumvent security features, or to utilize this system for other than its intended purposes are prohibited."

⁴⁹⁷ Paragraph 2-5a(3) in AR 380-53, the computer-monitoring regulation, requires "all computers attached or accessible through government-owned or -leased telecommunications networks" must display the prescribed access warning banner. This banner is employed at the logon or authentication step, as AR 380-53 requires the banner to "be placed on the computer in such a way that the user must press a key to get beyond it, thereby demonstrating his or her acceptance of its provisions." IAW AR 380-53, the access warning banner is not required on stand-alone computers not connected to the Army's telecommunications networks, and it doesn't apply to publicly accessible, non-restricted Army WWW sites – those sites employ the security warning banner from the DoD Web policy. The notice and consent banner (approved by the DoD CIO to be used on all DoD Websites that require logon / authentication) in Paragraph 4.2, Part V, and AR 25-2's banner are identical.

security measures (e.g., authentication and access controls) to protect USG interests – not for your personal benefit or privacy. Notwithstanding the above, using this IS does not constitute consent to PM, LE, or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.”

See Appendix L for templates on required statements.

Required links. The following are required links:

- Major organizational pages like HQ TRADOC must link to USA.gov from their homepage. The entry for the link is to read “USA.gov: U.S. Government Web Portal.”⁴⁹⁸ Unless the organization is Army, Army-command or HQ DA-staff-element level, a link to USA.gov is not required.
- To improve Website utility, each Webpage must link back to the Website’s homepage and to its parent organization’s homepage. All TRADOC sites must link to the next senior Website in the hierarchy IAW TR 10-5; the organizational homepage on AKO if one exists; the TRADOC logo and motto; the HQ TRADOC homepage; and the Army homepage.⁴⁹⁹ HQ TRADOC will link back to the Army homepage (www.army.mil). If an organization uses a graphical link, that link must also contain text indicating that it links back to the homepage.⁵⁰⁰
- A link to the FAQ page must be provided from the “About Us” page.
- A link to the portal for most frequently requested publication(s) must be provided from the “About Us” page.
- A link from the homepage must be provided to the “Help” page.

See Appendix L for a template on public-policy statements about hyperlinks.

Required Webpages.

“Important Notices” page. Because all Army Websites must be in compliance with Section 508 and must provide a link to the organization’s accessibility policy from the “Important Notices” page,⁵⁰¹ all TRADOC organizational Websites, not just HQ TRADOC, must include an “Important Notices” page. A link to this page must be placed at the footer of every Webpage. The “Important Notices” page describes principle policies and other important notices that govern the Website, especially those mandated by law. At a minimum, this page includes:⁵⁰²

- The privacy and security policy,⁵⁰³ including the cookie policy. The cookie policy must state that the Website is free of persistent cookies or other devices designed to collect PII about Web visitors, as the DoD standard notice included in Appendix D, this *Guide*, does. The privacy / security notice describes how security is maintained on the site, what specific information is collected, why it is collected, how it is used, whether disclosure is mandatory or voluntary, and the consequences of not providing the information.⁵⁰⁴ All information collected must be described in this notice. The legal rights of individuals, as guaranteed by federal laws, regulations, and policies, must be protected when collecting, maintaining, using, or disseminating personal information about individuals.⁵⁰⁵

⁴⁹⁸ Paragraph 8-5d, DA PAM 25-1-1.

⁴⁹⁹ Paragraph 5-5b(1), TR 25-1.

⁵⁰⁰ Paragraph 8-5c, DA PAM 25-1-1.

⁵⁰¹ Paragraph 8-3b(2), DA PAM 25-1-1.

⁵⁰² Paragraph 8-2f(2)(k), DA PAM 25-1-1.

⁵⁰³ The requirements for the privacy and security notice are also described in Paragraph 6-7c(5), AR 25-1: “Websites will display a privacy and security notice in a prominent location on at least the first page of all major sections of each Website. Each privacy and security notice must clearly and concisely inform visitors to the site what information the activity collects about individuals, why it is collected, and how it will be used. For an example, see the DefenseLink Website (official Website of DoD), which states, ‘For management purposes, statistical summary information or other non-user identifying information may be gathered for the purposes of assessing usefulness of information, determining technical design specifications, and identifying system performance or problem areas.’ Persistent ‘cookies’ that track users over time and across different Websites to collect [PII] are prohibited on public Websites. The use of any other automated means to collect [PII] on public Websites without the express permission of the user is prohibited. Requests for exceptions must be forwarded to the Army CIO/G-6. Third-party cookie generation will be disabled.”

⁵⁰⁴ Paragraph 4.2.2, DoDD 5400.11.

⁵⁰⁵ Paragraph 4.1.2, DoDD 5400.11.

- How to request information under FOIA. Website visitors should be advised how to make FOIA requests, including local contacts and by emailing FOIA@rmda.belvoir.army.mil.
- Accessibility (Section 508) policy. Text should advise Website visitors that it is the Army's policy that its Websites are accessible to handicapped users IAW Section 508 of the Rehabilitation Act; describe the organization's compliance with Section 508; and inform visitors whom to contact for a Section 508 complaint.⁵⁰⁶
- QI guidelines. Website visitors should, at minimum, be advised that the organization's goal for its on-line information is accuracy, objectivity, and integrity, and that it undergoes technical, supervisory, editorial, or legal review, as appropriate, based on the information's nature. Website visitors should also be given the generic contact information for the organization's QI POC.

Links to other Webpages containing this information are acceptable (and in several cases, are desirable to avoid repetition, such as the content required on the "Contact Us" page), as long as the "Important Notices" page consolidates the links required in the preceding bullets.

"Contact Us" page. Each Website must post a "Contact Us" page and provide links to it from the homepage and every major point of entry on the Website. The page must be labeled "Contact Us" or "Contact [organization name]" and contact information will be generic. Army policy⁵⁰⁷ requires these specific items of content on the "Contact Us" page:

- Organization street address, including addresses for any regional or local offices.
- Office phone numbers, including numbers for any regional or local offices.
- Means to communicate via email – organizational email (not by-name email) or Web-based contact form. (See requirements for a Privacy Act statement (PAS) or privacy advisory (PA) in Appendix D.)
- Organization's policy and procedures for responding to email inquiries, including whether the organization will answer inquiries and expected response time.
- Contact information for the organization's QI Program POC.
- Contact information (title/phone number) for small businesses (required by the PRA).
- Means to request information through FOIA – also included on "Important Notices" page – provide local contact and instruct visitors to make FOIA requests by emailing FOIA@rmda.belvoir.army.mil.

"About Us" page. Main-entry-point Websites such as the Army, USAR, ARNG, and ACOMs must post an "About Us" page. TRADOC commands / activities may provide links to HQ TRADOC's "About Us" page alongside their TRADOC homepage links, or they may establish a page on their own servers mirroring TRADOC's page, but they should do one or the other. The page must be labeled "About Us" or "About [organization name]." The organization will include at least all of these specific items of content on the "About Us" page:⁵⁰⁸

- Description of the organization's mission, including its statutory authority.
- The organization's strategic plan (unclassified, non-sensitive, or non-critical-information version), vision, or set of principles.
- The organization's structure, including basic information as well as parent and / or subsidiary organizations and regional and field offices.
- Contact information, which may include generic email address, phone number, office, title, or position.
- Information about jobs and other professional opportunities at the organization – the preferred method is to link to Civilian Personnel On-line (CPO) at <http://acpol.army.mil/employment/index.htm>.

Sitemap or subject index page. Each Website must include a sitemap or subject index that gives an overview of the Website's major content categories. At minimum, the sitemap must be linked from the homepage.⁵⁰⁹

⁵⁰⁶ Paragraph 8-3, DA PAM 25-1-1.

⁵⁰⁷ Paragraph 8-2f, DA PAM 25-1-1.

⁵⁰⁸ Paragraph 8-2f(2), DA PAM 25-1-1.

⁵⁰⁹ Paragraph 8-2f(2)(f), DA PAM 25-1-1.

FAQ page. Each Website must post a frequently asked questions or “common questions” page that provides basic answers to questions the organization receives most often.⁵¹⁰

“Help” page. Each Website must furnish a “Help” page that outlines major proposed and implemented changes to the Website.⁵¹¹

“The government should use social media, not just to create transparency, but also to help people accomplish their core tasks. ... To do this, the government must ensure that federal employees who need access to social-media tools have them, and that these new ways of delivering content are available to all, including people with disabilities. The new [a]dministration should develop government-wide guidelines for disseminating content in universally accessible formats (data formats, newsfeeds, mobile, video, podcasts, etc.), and on non-government sites such as YouTube, Wikipedia and SecondLife. To remain relevant, government needs to take our content to where people already are on the Web, rather than just expecting people will come to government Websites. Having guidelines will ensure that we’re part of the larger ‘on-line information ecosystem’ without compromising the integrity of government information.” – **Putting Citizens First: Transforming On-line Government**, Federal Web Managers Council whitepaper

Search page or search box. Organizations must include either a search box or a link to a search page from every page of the Website. The search box or link will be entitled “Search.”

Webmasters will place subject and keywords in source code to aid content searches. Focused searches may be given to search within sets of information, databases, or applications. Websites that are narrow in scope or less than 200 pages may substitute a sitemap or A-to-Z subject-index search rather than implement a search engine.⁵¹² Or, a Website can offer a search engine, sitemap, and A-to-Z search like the Army Website, www.army.mil, does.

See Appendix L for templates on Webpages that the Army requires. The text contained in those templates is suggested for adoption and will fulfill Army requirements if followed. In cases where the precise text is required, that will be noted.

General required content.

Easy access to customer services. Each Website must provide easy access to on-line customer services and forms applicable to the general public, displayed as prominently as possible, and based on an analysis of customer needs.⁵¹³

Portal to most frequently requested publications.⁵¹⁴ Each organization’s general-public Website must provide a link to the organization’s portal for its most frequently requested publication(s). This portal, which will be set up IAW TRADOC G-6 guidelines for portals as content not appropriate for the general public, will contain publications useful to the organization, and will be on the organization’s AKO site rather than on its general-public Website. The general-public site, as stated, may contain links to useful publications on APD’s on-line site.

POLICY: SECTION 508 COMPLIANCE

Army Websites must comply with Section 508 of the Rehabilitation Act, designed to make on-line federal-government information and services fully available to disabled employees and to members of the public with disabilities. Access for disabled persons must be comparable to the access available to non-disabled persons. DoD Web policy and Army regulation requires

organizational Webmasters and content managers (PAO) to be responsible for ensuring their Webpages are Section 508 compliant (IAW Subsection 1194.23).⁵¹⁵

Section 508 applies to electronic and information technology (EIT), which includes computers and networks, hardware, software, Webpages, and email, as well as equipment such as telecommunications and / or office

⁵¹⁰ Paragraph 8-2f(2)(g), DA PAM 25-1-1.

⁵¹¹ Paragraph 8-3b(10), DA PAM 25-1-1.

⁵¹² Paragraph 8-3b(8), DA PAM 25-1-1. The paragraph also outlines minimum service-level standards for the search function.

⁵¹³ Paragraph 8-2f(2)(h), DA PAM 25-1-1.

⁵¹⁴ Paragraph 8-2f(2)(j), DA PAM 25-1-1.

⁵¹⁵ Paragraph 3e, DoDD 5122.05; Paragraph 4k, DoDD 8000.01; Paragraphs 6-1p and 6-7a(14), AR 25-1; Paragraphs 7-5a, 8-3a and 8-3b(2), DA PAM 25-1-1.

equipment – e.g., equipment used for transmitting, receiving, using, or storing information such as fax machines, copiers, and telephones.⁵¹⁶ EIT also includes multimedia as well as information kiosks.⁵¹⁷

Paragraph 4k, DoDD 8000.01, gives an exception: “unless an undue burden would be imposed.” A federal agency does not have to comply with technology-accessibility standards in **procurement** if it imposes undue burden, which is defined as significant difficulty or expense. When applying for undue burden, the organization must explain why meeting standards would pose undue burden and must still provide people with disabilities access to information or data that’s affected. And, the kicker is that undue burden does not apply to Webpages, only procurement.

All new and / or updated Webpages, as well as all downloadable files (for example, PowerPoint slides, Portable Document Format (PDF) documents, and Microsoft Word documents), must be Section 508 compliant before they are posted, regardless of security controls in place. If a particular file to be downloaded cannot be made accessible to users with disabilities, then the content should be put in an accessible format and posted to the Web along with the original content. Go to <http://www.section508.gov> for information on this policy. For more information on making PDF files accessible to people with disabilities, go to <http://access.adobe.com/>.

Offices of primary responsibility (OPRs) are responsible for ensuring their multimedia / VI productions comply with both Section 508 and DoD guidance and therefore have captioning for the hearing-impaired.⁵¹⁸

See Appendix N for accessibility standards.

Army Webpages must support the widest possible range of users. Webpages should use a high-contrast color scheme to promote and support readability by all users. The standard background color for Webpages should be white, with dark-colored text, preferably black.

Other visitor-usability tips include:

- Webpage authors should use images only when necessary, as a number of images on a Webpage use more bandwidth but also decrease usability for disabled persons. A half-dozen small images will slow down a Webpage load as much as a single large one. Webpage authors should design Webpages around the information, not the graphics.
- We recommend that Webpage graphics be no more than 535 pixels wide or 320 pixels high, or visitors with small computer screens will have to scroll. A rule-of-thumb for individual graphics is a file size no larger than 50 kilobytes. (There are exceptions, such as high-resolution, large images intended for on-line delivery to printing, as is common with news services.⁵¹⁹) Large graphics should be kept off-line. If a Webpage includes a large graphic file, the Webpage author should provide a hypertext link or a low-resolution thumbnail image link to it rather than displaying it on the Webpage.
- Webmasters should use the “height” and “width” attributes as additions to the basic image-source tag for best performance: . This includes all button navigation graphics. Images should also have a useful description written behind the ALT tag to enhance Section 508 compliance.

“Agencies are required to provide on-line information that’s readily accessible by people with disabilities, as well as to people with limited English proficiency. However, few agencies have the funding, training or resources to meet these obligations. The government should establish standards and guidelines for multilingual Websites, and agencies should be funded and staffed with qualified bilingual Web-content professionals who can create and maintain them. This will help newcomers learn about the rights and responsibilities of living in the United States.” – **Putting Citizens First: Transforming On-line Government**, Federal Web Managers Council whitepaper

Having accessible Websites may be critical to our wounded warriors attempting to do a job in support of our Army. According to **Stand-To!** March 24, 2009, many Soldiers sustain multiple injuries and require a combination of assistive-technology devices, plus accommodations and training for conditions involving dexterity, cognitive

⁵¹⁶ Paragraph 6-1p, AR 25-1.

⁵¹⁷ Paragraph 6-1p, AR 25-1; Paragraph 7-5b, DA PAM 25-1-1.

⁵¹⁸ Paragraph 7-7a(6)(b)7, AR 25-1.

⁵¹⁹ News services are provided by the PAO for its organization, such as the command-wide news service established by major Army command PAOs for their subordinate organizations. See Paragraph 3-5d, AR 360-1.

difficulties (including traumatic brain injury), vision loss, and hearing loss. Examples of the technologies wounded warriors use may be applied to their use of Websites: screen readers, cueing and memory aids, magnification software, voice-recognition software, assistive listening devices, voice amplifiers, alternative keyboards, and pointing devices.

TRADOC PAO recommends that Webpage authors check their Webpage's Section 508 compliance via the W3C's free validator at <http://validator.w3.org>, then manually check the page, since automated validators will not catch everything or may come back with false non-compliance results. If not using the W3C's validator, Webmasters / portal administrators should validate accessibility of Websites / portals with another automated tool and with human review. Automated methods are generally rapid and convenient but cannot identify all accessibility issues, according to the W3C; human review in addition to automated review can help ensure clarity of language and ease of navigation.

To ensure Section 508 compliance IAW AR 25-1, requests for content review submitted to PAO should include a verification summary / results generation from a W3C-approved automated tool. The 508-compliance results as determined by the tool, along with the comments from human review, will be sent through the content-review process outlined in Chapters 2 and 3, along with other required materials, before the content / page will be approved for posting. **No TRADOC Webpage may be approved for posting, however, if it contains Priority 1 accessibility errors as defined by the W3C.** (Priority 1 errors are errors determined by the W3C to seriously affect Webpage usability by people with disabilities. See <http://www.w3.org/TR/WCAG10/> for more information.)

It may be hard to understand why complying with Section 508 isn't "undue burden," so we'll make some points that can be stressed to organization members who need "motivation."

Section 508 compliance is good for the command because compliance enables the installation's own civilian workforce.

- Disabled people are not "they" – they're us: our civilian workforce, our retirees, our taxpayers, our wounded warriors, ourselves – if not now, then perhaps someday.
- The civilian workforce uses the WWW at times to do their jobs. Retirees and taxpayers use a command's Website to seek information about the command and installation.
- People with disabilities are the largest minority in the United States. (African-Americans are the second largest minority with 12.8 percent of the population.) The 1997 U.S. Census Bureau report on Americans with disabilities found that 52.6 million people (19.7 percent of the population) had some level of disability, and 33.0 million (12.3 percent of the population) had a severe disability.
- Many of those disabled adults are vision impaired: 7.67 million adults have difficulty seeing words / letters; 3 million people are color blind; 1.77 million adults report severe vision impairment.
- A significant number are hearing impaired: 8 million adults have difficulty hearing a conversation; 832,000 report a severe hearing impairment; 3.9 million adults use a hearing aid.
- The largest percentage of disabled adults are mobility impaired: 19.5 million adults have difficulty walking; 9.9 million report a severe mobility impairment; 8.53 million use a wheelchair, crutches, or a cane.
- Another significant percentage of disabled adults are those with limited hand use: 18.1 million adults report difficulty grasping or carrying objects; 8 million report severe difficulties.
- 3.5 million adults have a learning disability; 9 million adults have cognitive disabilities.
- When there are post-war-on-terror statistics available, the percentage of disabled adults, especially the youngest age bracket (see below), will increase.
- Given the preceding statistics, a non-compliant Website will most likely affect an Army civilian with vision impairment (such as difficulty distinguishing colored type that's close in color to the Webpage background) or limited hand use (for instance, if navigation requires dexterous use of the computer mouse, such as flowing menus often do). A non-compliant Website may hamper these workers in doing their jobs.
- Aging increases one's chances of disability, as might be expected, but the statistics don't show that disability is restricted to *old* age. A significant number of middle-aged people are disabled. According to the Census Bureau, in the age 25-44 bracket, 13.4 percent of the population reports having any type of disability, while 8.1 percent reports a severe disability, but the numbers rise significantly for the age 45-54 bracket. This group has 22.6 percent reporting any type of disability, with 13.9 percent having a severe

disability. As your installation's civilian workforce reaches retirement age, they could be in the company of the age 55-64 group, with 35.7 percent having any type of disability and 24.2 percent a severe disability.

- Not forgetting the retiree population your installation Website may serve, age group 65-69 reports 44.9 percent as having any type of disability, with 30.7 percent having a severe disability; between 70-74, 46.6 percent have any type of disability and 28.3 percent have a severe disability; in the 75-79 bracket, 57.7 percent have any type of disability and 38.0 percent having a severe disability; age 80 and over, 73.6 percent have any type of disability, while 57.6 percent have a severe disability.

Just what is a "disability"? By definition, a person is considered to have a disability if he or she has difficulty performing certain functions (seeing, hearing, walking, climbing stairs, and lifting and carrying), or has difficulty performing activities of daily living, or has difficulty with certain social roles (doing schoolwork for children, working at a job and around the house for adults). A person who is unable to perform one or more activities, or who uses an assistive device to get around, or who needs assistance from another person to perform basic activities, is considered to have a severe disability.

Section 508 compliance is good for the command because compliance will lead to Websites that are better designed and more friendly to technology used by employees who are TDY. These better Websites will also produce goodwill from the public.

- Section 508 compliant Websites are usually better designed than non-compliant ones. If a Webpage author remembers that not everyone views a Webpage the same way he / she does, he or she is more likely to create a Webpage with more user-friendly navigation, better contrast of text to background, and less chance of something going wrong such as browser or plug-in incompatibility (and therefore content being lost to the Webpage visitor).
- Creating an accessible Webpage is creating a page that is interoperable, platform-independent, and functional for everyone. Webpages for anyone can benefit from Section 508 compliance, since the spirit of accessibility is providing the information in a format anyone can easily understand.
- Websites that are Section 508 compliant are normally more easily used by TDY employees using laptops, PDAs, or Internet-enabled pages and phones. Deployed Soldiers may face slow dial-up connections or primitive geographical areas; Section 508 compliance will enable them to access the command's Website more easily.
- Section 508 compliant Websites are clear to people who have turned off graphics for faster page loading.
- A Section 508 compliant Webpage is not plain text. In fact, some people rely on graphics to help them understand a Webpage's content, so images are necessary for Section 508 compliance in those cases.
- An installation Website that provides a pleasant experience for the user is more likely to induce public goodwill.

Some last notes for this section:

- Care with HTML writing can go a long way in making Websites Section 508 compliant. For instance, Websites often have a splash or homepage heavy on images, and those images often fail to have ALT text in the graphic's HTML tags. Graphical buttons fail to offer alternate text links. Now imagine you are blind – your screen reader cannot read text on the buttons (it's part of the image) and would not find a clue in the HTML about what the big piece of art is at the page's top. The spirit of Section 508 is equal access. You are supposed to create ways for a blind person to have a sighted person's experience of the page by describing in the ALT text what the banner image portrays. Not having ALT text for graphical navigation buttons does not give a blind person the same navigation access as to a sighted person. To make buttons with words on them Section 508 compliant, the Web designer must provide a text hyperlink.
- While manufacturers are required to achieve Section 508 compliance in their software, insisting on Braille access isn't necessary. Good screenreaders adapt well to properly written HTML pages; Braille access is made on the blind person's end (his / her keyboard) and not on the software-on-the-server end. Again, the consideration is that to be Section 508 compliant, there should be a text alternative to PDFs and images.
- Where to look for the compliance standards may be confusing. The foundational document is Sub-section 1194.22 of Section 508, which covers Web-based intranet and Internet information and applications. At one time, DoD adapted this section to its 13 Web-accessibility rules that matched up with the Section 508

standards and some of the Priority 1 checkpoints in the W3C's Web Content Accessibility Guidelines (WCAG) 1.0. However, WCAG 2.0, the current version, is quite different; nothing correlates exactly among these references anymore; and a content reviewer's / Section 508 compliance researcher's best bet is to refer to DA PAM 25-1-1, where the standards are specified for the Army – see Appendix N.

POLICY: OTHER POLICY AND GUIDANCE

In addition to where elsewhere stated, information must also meet the Website management-control checklist items in Paragraph C-4, Appendix C, AR 25-1, test questions 25 through 34,⁵²⁰ and other DoD, Army, and TRADOC policies and guidance. Website coordinators / Web-content managers and content reviewers must answer these test questions by actually testing the management controls. G-6 and PAO content reviewers should notify content providers of “no” responses to Paragraph C-4's test questions and other policy violations when answers to the test questions indicate deficiencies. Content providers may be expected to explain deficiencies to G-6 and PAO content reviewers, and to indicate their corrective action in their supporting documentation.⁵²¹ As discussed in previous chapters, Website coordinators / Web-content managers, content reviewers, and content providers are responsible for knowing and applying DoD / Army / TRADOC policies and guidance.

“Agencies should receive adequate resources to make their Websites fully accessible to people with disabilities and meet requirements of the Rehabilitation Act. The new [a]dministration should invest in government-wide solutions, such as captioning software to make videos and webcasts accessible to people with disabilities.” – **Putting Citizens First: Transforming On-line Government**, Federal Web Managers Council whitepaper

The key management controls must be formally evaluated at least once every five years.⁵²²

Official Websites are prohibited from displaying sponsorships or commercial advertisements: “Commercial sponsorships, advertisements, and endorsements are prohibited on publicly accessible pages of official DoD Websites. Publicly accessible Websites are official communications to the public. ... Organizations shall ensure that the credibility of official information is not adversely affected by association with commercial sponsorships, advertisements, or endorsements.”⁵²³

Advertising implies endorsement, which is prohibited by Paragraph 3-209 of the JER: “Endorsement of a non-federal entity, event, product, service, or enterprise may be neither stated nor implied by DoD or DoD employees in their official capacities.” In the same spirit of non-endorsement, no icons can be used for links to non-Army software download sites – Webmasters may use only text or hyperlinked text.

TRADOC Websites may contain no advertising, nor link to a non-TRADOC site if the non-TRADOC site is posted with advertising.

The issue of endorsement also underlies AR 360-1's guidance on election-year policies.⁵²⁴ These policies will guide PAO treatment of information and release via command Websites and newspapers, as “[g]enerally, DoD does not

⁵²⁰ Paragraph 8-4a, DA PAM 25-1-1, refers to Paragraph 6-4n (now Paragraph 6-7) and Appendix C-4 of AR 25-1 as Army policy. Since Paragraph C-4, Appendix C, AR 25-1, is set up in the form of questions, reviewers will consider “no” responses to test questions 25 through 34 as violations of Army policy established for OPSEC, personal privacy, other sensitive information, pre-decisional information, FOIA-exempt information, copyrighted information, commercial sponsorship, and advertising, or other policy. We suggest test questions 1, 2, and 7 in Paragraph C-4g as applicable policy for record-keeping procedures for organizational Websites.

⁵²¹ Paragraph 9-1e(2)(c), DA PAM 25-1-1.

⁵²² Paragraph 9-1e(2)(c), DA PAM 25-1-1.

⁵²³ Paragraph 9, Part II, DoD Web policy. See also DoDI 8410.1: “Websites and other Internet media in domains specifically funded by, registered to, or exclusively used by [DoD], and visible to or distributed to the public, shall not be used to advertise or market private individuals, commercial firms, corporations, or not-for-profit firms. Such media must not imply in any manner that [DoD] endorses or favors any specific commercial or not-for-profit product, commodity, or service.” And Paragraph 3-5m, AR 360-1: “No private non-government organization or association will be favored over another in PA products.” AR 25-1 also discusses non-endorsement practices – IAW Paragraph 6-4r(1), AR 25-1, installations may publish directories separately, as a subsection of a local installation guide published by PAO, and further, combination installation guides and installation directories may contain commercial advertising *separate* from the directory section. IAW Paragraph 6-4s(10), AR 25-1, since the Army must avoid both the fact and the appearance of underwriting a commercial television service, program materials for use on CI stations, provided by its commercial-television-service franchisee, may not contain commercial advertising or announcements.

⁵²⁴ Paragraph 3-4, AR 360-1.

engage in activities that could be interpreted as an association with any partisan political causes, issues, or candidates.”⁵²⁵

- Consider inquiries from political-campaign workers as queries from the general public and provide only information / material available to the general public.⁵²⁶
- When a candidate for political office is invited to participate in official business, the candidate may appear on camera and in photographs as an official participant, and may make a statement or answer questions about the official business being conducted. A candidate may *not* receive approval to make a campaign- or election-related statement or to respond to a campaign or election-related media query.⁵²⁷
- To avoid the appearance of preferential treatment, all candidates for national office who are not current members of Congress or serving governmental officials should be offered the same access to installations as any other unofficial visitor.⁵²⁸
- DoD Public Affairs broadcast activities and publications, both Army-funded (AF) and civilian enterprise (CE), will support the Federal Voting Assistance Program (FVAP) by carrying factual information about registration and voting laws, specifically information on absentee voting requirements and key submission and cutoff dates for the various states and territories.⁵²⁹

The scope and definition of an election time period may be more extensive than some realize, as a political campaign or election begins when a candidate, including an incumbent office- holder, makes a formal announcement that he / she seeks to be elected to a federal, state, or local political office. A political campaign or election also begins when an individual files a candidacy with the Federal Election Commission (FEC) or equivalent state or local regulatory agency. Once initiated, a political campaign or election does not end until one week after the conclusion of the relevant election.

POLICY: INSTALLATION NEWSPAPERS ON THE WEB

For PAOs who have gotten “nasty-grams” about policy violations regarding some aspect of your newspaper operations, this section may be of interest. If your newspaper is on the dot-mil domain, it must comply with all Army and DoD policy. However, if your CE publisher posts your newspaper to a commercial domain, some of the policy may not apply. We’ll explain.

If your newspaper is posted on the dot-mil, the policy is:

- Army-funded newspapers and the editorial content of CE publications may be posted on Websites but must comply with DA PAM 25-1-1, Paragraph 8-2h: “Although generally public domain, [Army installation newspapers] are part of the Army internal information program. While publishing installation or organization newspapers constitutes public release of information, the distribution is limited. Publishing on an unlimited-access Website represents global release. Some information appropriate for installation newspapers is not appropriate for public Websites. Army organizations may reproduce the content of installation newspapers for the Web if that content meets the restrictions provided in AR 25-1. These restrictions include prohibitions against posting names, locations, and specific [PII] about employees and military personnel and their family members. Advertisements appearing in private-sector newspapers should not be posted on Websites.” Therefore **PII is limited in newspaper content on the dot-mil, and there can be no advertising.**
- “The policies and procedures in DoDI 5120.4 apply to all DoD newspapers and CE publications, whether printed or electronic. DoD-funded newspapers and editorial content of CE publications may be posted on DoD Websites without advertising.”⁵³⁰
- All information residing on a publicly accessible Website is public information, even if it is intended for an internal audience – as in the case of installation newspapers – and is subject to Army policies and clearance procedures.⁵³¹

⁵²⁵ Paragraph 3-4a, AR 360-1.

⁵²⁶ Paragraph 3-4b, AR 360-1.

⁵²⁷ Paragraph 3-4c, AR 360-1.

⁵²⁸ Paragraph 3-4c, AR 360-1.

⁵²⁹ Paragraph 3-4d, AR 360-1.

⁵³⁰ Paragraph 7.3, Part II, DoD Web policy.

⁵³¹ Paragraph 13-14, AR 360-1; Paragraph 6-7c(3), AR 25-1.

- DoD policy requires that both DoD publicly accessible and access-controlled Internet-based communications (such as email or Webpages) be conducted on the .mil domain,⁵³² and that no .mil domain name redirects to a non-.mil host.⁵³³ Non-residence on the .mil or .gov domain must be approved as a waiver by the Army CIO / G-6 and must be IAW the exceptions listed in Enclosure 3, DoDI 8410.1.⁵³⁴
- Army organizations using non-dot-mil domains to post official content must transition their Websites to the army.mil domain.⁵³⁵

If you've gotten a notification that your installation newspaper, posted by your CE publisher to its site, is in violation of a provision quoted from AR 25-1, there are **six key things you should know**:

- Discuss this with your SJA, but AR 25-1 may not apply. AR 25-1 outlines requirements and policy on the use of **government-owned or -leased computers**, including those computers' access to the Internet.⁵³⁶ AR 25-1's applicability is limited to "IT contained in command-and-control (C2) systems, intelligence systems (except as noted), business systems, and (when identified) national-security systems (NSS) **developed or purchased by [DA]**."⁵³⁷ The critical phrase, of course, is "developed or purchased by [DA]." Because, if you've adhered to DoDI 5120.4 and AR 360-1, the paginating and processing workstations that the CE publisher has placed in your office are owned and maintained by that CE publisher, and therefore the IT is not DA's.⁵³⁸ In fact, you're *prohibited* from buying IT, using either appropriated or non-appropriated funds, to "pay for any part of a CE publisher's costs incurred in publishing a CE publication."⁵³⁹
- However, you must ensure network security, as AR 25-1 and AR 25-2 are clear: "The only authorized access from Army ... networks to the Internet is through a DISN-controlled and -monitored connection."⁵⁴⁰ Your CE pagination system or other CE IT is "unofficial communications" – it **must be isolated, either logically or physically**, from official DoD and Army NIPRNET networks.⁵⁴¹ Supervisors and managers are charged to ensure that there are no cross-connections directly between the Internet and NIPRNET of non-Army-owned ISs.⁵⁴² (Supervisors and managers may allow direct connections to the Internet to support electronic commerce when systems will not connect to the NIPRNET or the SIPRNET; see Paragraph 4-20d, AR 25-2, for security measures to apply between enclaves.)
- The line for transmitting "electrons" back and forth to the CE publisher is borne by the CE publisher, of course, and AR 25-2 authorizes this as long as, again, no cross- or direct connectivity to the NIPRNET exists or will be implemented.⁵⁴³ Commercial ISP services are authorized to support organizations identified in Paragraph 4-20b(2), AR 25-2, which are "proponents for programs that require network services for family members, retirees, and other individuals serviced at Army installations."⁵⁴⁴ As these groups are historically audiences for installation newspapers, authorization under AR 25-2 should not be an issue.

Arguing the non-applicability of AR 25-1 to CE newspaper operations is far more preferable than trying to get a waiver under AR 25-1's Paragraph 6-7b, which will likely be an exercise in futility. In discussing that the use of the army.mil domain is required for sites on the NIPRNET and SIPRNET, the AR says a waiver may be granted for "special needs." You may try to fit under the category of "specialized services on contracted commercial systems not connected to the NIPRNET or SIPRNET and not reliant on access-control mechanisms used in the ".mil" domain," but among the things you have to justify in your waiver request is that there will be "confirmation that

⁵³² Paragraph 4a, DoDI 8410.1.

⁵³³ Paragraph 4d, DoDI 8410.1.

⁵³⁴ Paragraph 1, Enclosure 3, DoDI 8410.1; Paragraph 6-7b(1), AR 25-1. Exceptions to the policy, examples of special needs or requirements that may be considered and approved for other than the army.mil domain, and the "how to" on submitting waivers is in Paragraph 6-7b, AR 25-1.

⁵³⁵ Paragraph 8-1d, DA PAM 25-1-1.

⁵³⁶ Paragraph 4-20g(1), AR 25-2.

⁵³⁷ Paragraph 1-1, AR 25-1.

⁵³⁸ Paragraph E4.1.5, 5120.4; Paragraph 13-5e(5), AR 360-1.

⁵³⁹ Paragraphs 6.2.4 and E.4.1.1, DoDI 5120.4; Paragraphs 3-5g and 13-5a, AR 360-1.

⁵⁴⁰ Paragraph 6-4o, AR 25-1.

⁵⁴¹ Paragraph 4-20b(2), AR 25-2.

⁵⁴² Paragraphs 4-20c(3) and (4), and 4-20g(6), AR 25-2.

⁵⁴³ Paragraph 4-20g(6), AR 25-2.

⁵⁴⁴ Paragraph 4-20b(2), AR 25-2.

there will be no association on the Website with the name of the private provider, no advertising, and no commercial trademarks or symbols.” This will be *highly* impossible because of the CE publisher.

- Also, commanders and heads of organizations are authorized to link to a commercial / civilian Website carrying the authorized CE publication, including its advertising, provided the **standard disclaimer for external links** is given.⁵⁴⁵ We infer from this that the CE publisher is “allowed” to have a Website with the authorized newspaper, and the post’s official site is allowed to link to it. Since the underlying premise of the CE concept is that DoD saves money by transferring certain publishing and distribution functions to a commercial publisher, we see the CE publisher’s posting of the installation newspaper on-line, along with the paper’s advertising, as the “**right to sell and circulate advertising** to the complete readership in the CE publication [to] provide the publisher revenue to cover costs and secure earnings,” as guaranteed by DoDI 5120.4. As part of the contract with the CE publisher, the command / installation should guarantee first publication and distribution of locally produced editorial content in the publication, including its Web version.⁵⁴⁶
 - An added benefit of on-line advertising, in addition to printed advertising, is the (hopeful) increase in installation-community communication, per DoDI 5120.4’s concept that “CE newspapers provide advertisements that guide command members to outlets where they may fulfill their purchasing needs. A by-product of this commercial contact is increased installation-community communication, which enhances mutual support.”⁵⁴⁷
- Another element of the policy and installation newspapers on the Web is that the CE newspaper is defined as an **authorized, unofficial publication**.⁵⁴⁸ In a number of communications about on-line installation newspapers, we’ve seen that G-6 has defined the newspaper site as an official Army site per AR 25-1, but it may be arguable that other policy says it’s not official.
- The sixth thing is that, per DoDI 5120.4, electronic publication of a CE publication is considered a **proper distribution outlet**.⁵⁴⁹ Following up with that is Paragraph 5-6c(6) in AR 360-1, which might be used to buttress the argument that since commanders must be aware of (and try to meet) the unique information needs of subgroups in the command, and since we know that the Internet is primarily where the 18-24-year-olds find their news, not having the CE paper on the Web most likely means that a major subgroup’s information needs will not be served.

In the end, it’s the commander’s decision. Although AWRAC is charged to continuously review the content of publicly accessible Army Websites to ensure compliance,⁵⁵⁰ it’s supposed to *advise* the commander on what corrective action needs to be taken.

Other policy dealing with installation newspapers or PAO (news service) sites on the Web:

- CE newspapers or Websites that are partnered with and have a primary client of the U.S. Army **may not carry paid political advertisements** or advertisements that advocate a particular position on a political issue. This includes the installation newspaper on a CE publisher’s site, even if the site is defined as unofficial.
- Whether on the CE site or on the dot-mil, releasable information must be accurate and must adhere to published DoD and Army policies.⁵⁵¹
- All **commercial advertising**, including advertising supplements, must be **clearly identifiable** as such. Paid advertorials and advertising supplements may be included but must be clearly labeled as advertising and readily distinguishable from editorial content.⁵⁵² (Although this provision is primarily applicable to the

⁵⁴⁵ Paragraph 7.3, Part II, DoD Web policy; Paragraph 4.21, DoDI 5120.4; Paragraphs 13-2i and 13-9i, AR 360-1.

⁵⁴⁶ Paragraph E4.1.10.1, DoDI 5120.4.

⁵⁴⁷ Paragraph 6.2.1.1.5, DoDI 5120.4.

⁵⁴⁸ Paragraph E2.1.2, DoDI 5120.4.

⁵⁴⁹ Paragraph E4.1.6.4, DoDI 5120.4: “Except as authorized by the next higher headquarters for special situations or occasions (such as an installation open house), CE publications shall not be distributed outside the intended DoD audience and retirees, which includes family members. Electronic publication on the Internet and/or [WWW] is not considered distribution outside the intended DoD audience.”

⁵⁵⁰ Paragraph 4-20g(16), AR 25-2.

⁵⁵¹ Paragraph 5-4b, AR 360-1.

⁵⁵² Paragraph 4.16, DoDI 5120.4; Paragraphs 13-2h and 13-9h, AR 360-1.

printed newspaper, remember that the “policies and procedures in DoDI 5120.4 apply to all DoD newspapers and CE publications, whether printed or electronic.”⁵⁵³

- Publications must distinguish between editorials (command position) and commentaries (personal opinion) by clearly identifying them as such.⁵⁵⁴
- In addition to on-line newspapers, CE publications consist of DoD printed newspapers, magazines, installation guides, installation maps, and Websites that support command internal communications.⁵⁵⁵ As part of the internal-communication mission, newspapers and magazines may publish community-service news and announcements from the civilian community for the benefit of command or installation personnel and their families.⁵⁵⁶ CE guidebooks are intended primarily for a commander’s internal newcomer audience.⁵⁵⁷ CE installation maps, considered an unofficial publication as well, are intended for visitors (the general public) as well as newcomers.⁵⁵⁸ The commander or PAO provides oversight and final approval authority for the publication’s editorial content: news, features, photographs, editorials / commentaries, and other materials used in a CE publication.⁵⁵⁹
- While CE personnel may recommend or provide material for use in the publication if approved by the commander or PAO (as the commander’s representative),⁵⁶⁰ news content in DoD publications must primarily be based on releases, reports, and materials provided by the DoD components and their subordinate levels, DoD newspaper staff members, and other government agencies.⁵⁶¹ Editorial contributions may include articles and products produced outside official channels (for example, by stringers or local organizations), providing that permission has been legally obtained and that the contributions do not otherwise violate provisions of AR 360-1.⁵⁶² Commercial news and opinion sources – such as the Associated Press (AP), United Press International (UPI), or the *New York Times* – are not normally authorized for use in DoD publications except as stated in Subsection 4.7, DoDI 5120.4.⁵⁶³
- While a publication’s editorial content is controlled by the installation, the advertising section – including its content – is the responsibility of the CE contractor. This does not mean that the PA staff abrogates its responsibility for **reviewing advertisements before they are published**; the PA staff retains the responsibility for doing so for the on-line version of the publication as well.⁵⁶⁴
- The CE newspaper’s advertising – including its supplements and inserts – is the property of the command, installation, or intended recipient once it is published, IAW the contract’s terms.⁵⁶⁵
- The **on-line version of the installation newspaper should include, on its landing page, a statement** that “DoD newspapers do not necessarily reflect the official views of, or endorsement of content by, DoD.”⁵⁶⁶
- The CE publisher may wish to restrict access to the on-line installation newspaper to dot-mil IP addresses because of this provision in AR 360-1 (although it primarily applies to non-DoD commercial publications): “Military installations and commands are usually considered non-public forums. Therefore, First Amendment rights do not guarantee or allow unrestricted distribution access by civilian publishers. Commanders must stipulate controlled distribution (by location and quantity) of all non-DoD commercial publications on their installations or risk losing this non-public forum status.”⁵⁶⁷

⁵⁵³ Paragraph 7.3, Part II, DoD Web policy.

⁵⁵⁴ Paragraph 3-5r, AR 360-1.

⁵⁵⁵ Paragraphs E2.1.2 and E4.1.1, DoDI 5120.4; Paragraphs 3-5c and 13-5a, AR 360-1. See Paragraph 6.2.1.1.8, DoDI 5120.4: “The newspaper exists to facilitate accomplishment of the command or installation mission. That is the only basis for the expenditure of DoD resources to produce them.”

⁵⁵⁶ Paragraph E4.1.4, DoDI 5120.4.

⁵⁵⁷ Paragraph 13-11b, AR 360-1.

⁵⁵⁸ Paragraph 13-11d, AR 360-1.

⁵⁵⁹ Paragraphs E2.1.2.1, E4.1.1 and E4.1.4, DoDI 5120.4; Paragraphs 3-5c, 3-5o, 13-5a, and 13-5d, AR 360-1.

⁵⁶⁰ Paragraphs E2.1.2.1 and E4.1.4, DoDI 5120.4; Paragraph 13-5b, AR 360-1.

⁵⁶¹ Paragraph 4.5, DoDI 5120.4.

⁵⁶² Paragraph 13-2a, AR 360-1.

⁵⁶³ Paragraph E4.1.4, DoDI 5120.4.

⁵⁶⁴ Paragraph 13-9a, AR 360-1.

⁵⁶⁵ Paragraph E2.1.2.1, DoDI 5120.4.

⁵⁶⁶ Paragraph E2.1.2, DoDI 5120.4.

⁵⁶⁷ Paragraph 3-8f, AR 360-1.

Website Coordinator / Web-Content Manager Checklist The first section includes DoD / Army Website principles to check, helping ensure compliance with DoD Webmaster policy, ALDODACT 11/06, AR 25-1, DA PAM 25-1-1, and TR 25-1. Use in addition to PAO checklist provided in Chapter 3. The second section checks Websites' employment of strategic communication. "Yes" answers to Section II's questions will help ensure the organization's Website displays corporate ethos; whereas on the other hand, for most questions, "no" answers will indicate non-compliance to DoD / Army / TRADOC policy.				
Name of Reviewer	Date of Review			
URL / Proposed URL	Organization Webmaster Name / Email Address / Phone Number			
Department / Organization Name	Content Provider Name / Email Address / Phone Number <u>OR</u> Web Content Working Group (WCWG) Representative Name / Email Address / Phone Number			
Issue / Concern	Yes	No	N/A	Notes / Comments
DoD Website user principles and procedures				
1. Does the Website conform to the privacy principle, where Army, DoD, and federal standards on contact(s) must be followed to ensure that sensitive personal or unit information has been removed from publicly accessible Websites?				The privacy principle establishes that DoD personnel not only have a right to privacy, but that releasing PII establishes risk to those personnel. PII is categorized as FOUO. OMB memo M-05-04; OMB circular A-130, Appendix I; OMB memo M-03-22.
2. Does this Website conform to the principle of accessibility, where federal employees and members of the public with disabilities must have access to and use of information and data that is comparable to the access and use by individuals who do not have disabilities?				See OMB M-05-04 and Paragraphs 7-5a, 8-3a, and 8-3b(2), DA PAM 25-1-1. For Q2's answer to be "Yes," Websites must have 100 percent compliance to Qs 2a through 2e.
2a. Is the Website Section 508 compliant?				
2b. Does the Website use plain language which considers the knowledge and literacy level of the typical visitor?				The principle of accessibility requires simple, clear language. See Paragraph 8-3b(3), DA PAM 25-1-1.
2c. Is the text gender neutral?				See Paragraph 8-3b(3), DA PAM 25-1-1.
2d. Is the Website accessible to persons who may be limited in English proficiency?				See Paragraph 8-3b(3), DA PAM 25-1-1, and EO 13166.
2e. Does the Website avoid using abbreviations / acronyms on the homepage? Are abbreviations / acronyms used on subpages spelled out upon first reference?				See Paragraph 8-2b(1), DA PAM 25-1-1.
3. Does this Website conform to the principle of information quality?				Federal standard; see OMB M-05-04; OMB Circular A-130; Paperwork Reduction Act; E-government Act. Websites must have 100 percent

				compliance to Qs 3a through 3g for the answer to Q3 to be "Yes."
3a. Has the organization sponsoring the Website issued information-quality guidelines to its content providers?				IAW Paragraph 7-7a, DA PAM 25-1-1.
3b. Has the organization established a mechanism for users to make complaints about lack of quality?				IAW Paragraph 7-7a, DA PAM 25-1-1.
3c. Does the organization annually report the number and nature of those complaints?				IAW Paragraph 7-7a, DA PAM 25-1-1.
3d. Does the organization perform, and have adequate documentation of, pre-distribution / pre-dissemination content reviews as part of the organization's QI Program?				IAW Paragraph 7-7d, DA PAM 25-1-1.
3e. Are the reviews done by people with diverse areas of expertise appropriate for the type of information?				IAW Paragraph 7-7d(3), DA PAM 25-1-1.
3f. Does the organization treat information quality as an integral part to every step in the development of information?				IAW Paragraph 7-7d(3), DA PAM 25-1-1.
3g. Does the organization copy-edit text in the pre-dissemination process to ensure there are no typographical, spelling, or grammar errors?				
4. Has the organization kept evidence of its Web content reviews, including QI, Section 508 validation, and OPSEC? (principle of records management)				Chapter 8, AR 25-1; OMB M-05-04; OMB Circular A-130; NARA guidance.
5. Does this Website conform to the principle of information value, where the information must be of value to Website visitors?				IAW Paragraphs 8-1b, 8-2e, and 8-2a, DA PAM 25-1-1. Visitors may include users from Army organizations, other government agencies, academies, the private sector, and citizens with an interest in the missions performed [Paragraph 8-2a], but information may not be exclusively for the use of Army personnel and / or for the organization's employees. For the answer to Q5 to be "Yes," the answers to Qs 5a through 5f must be "Yes."
5a. Does the information on the public Web include the public at large?				
5b. Is all information that is for Army personnel only on AKO or placed on an approved intranet site IAW TR 25-1?				IAW Paragraph 8-1a, DA PAM 25-1-1.
5c. Is content the main focus for the target audience(s), rather than splashy graphics / "cool" design?				IAW Paragraph 8-2d, DA PAM 25-1-1.
5d. Does content serve as a general index to all major options available on the Website?				IAW Paragraph 8-2d, DA PAM 25-1-1.
5e. Has the Website's homepage minimized extraneous content to allow visitors to get to the content it needs and wants most?				IAW Paragraph 8-2d, DA PAM 25-1-1.
5f. If information is included that is meant exclusively for the organization's employees, is it for emergency or other exceptional situations?				IAW Paragraph 8-2e, DA PAM 25-1-1.
6. Does this Website conform to the principle of accurate official information, where the information available on the public Web must be accurate official information, regardless of whether the site is linked only to other government Websites but also to private-				IAW Paragraph 8-1b, DA PAM 25-1-1. This principle makes it an organization's responsibility to ensure its links to other sites, including to private-sector sites,

sector Websites?				also have quality information.
7. Does this Website conform to the principles on quality and governance of hyperlinks?				Federal standard; see OMB M-05-04; OMB Circular A-130; Paperwork Reduction Act; E-government Act. Also IAW Paragraph 8-1k, DA PAM 25-1-1. Answers to Qs 7a through 7g must be "Yes" before the answer to Q7 can be "Yes."
7a. Does the Website use only text or hyperlinked text (no graphics / logos) to direct users to non-Army software download sites?				IAW Paragraph 8-1k, DA PAM 25-1-1.
7b. Has the organization established, and does it enforce, explicit linking policies that describe its management controls for linking within and beyond the organization?				IAW Paragraph 8-1k, DA PAM 25-1-1. External links must be chosen fairly and in the best interest of the public.
7c. If so, does the Website contain a Webpage, or a link to a Webpage, that explains the process for linking to non-Army sites and includes guidelines for selecting and maintaining external links?				
7d. Does this explanatory Webpage explain why some links are chosen and others are not?				
7e. Does the Website's decision to link to an external source exhibit sound public policy and support the Army's mission?				IAW Paragraph 8-1k, DA PAM 25-1-1.
7f. Does the Website avoid making links to a political campaign, committee or lobby?				IAW Paragraph 8-2b(2), DA PAM 25-1-1.
7g. If the organization is using frames to link to external sites, has the organization consulted legal counsel concerning trademark and copyright issues?				IAW Paragraph 8.1.5, Part II, DoD Web policy.
8. Does this Website conform to the principle of proper labeling?				IAW Paragraph 8-1j, DA PAM 25-1-1. Answers to Qs 8a and 8b must be "Yes" before the answer to Q8 can be "Yes."
8a. Are draft policies, regulations or other pre-decisional information removed from publicly accessible Websites?				
8b. Is copyrighted information labeled with the owner's copyright attribution, and does the organization have written permission to post the information from the copyright owner?				
9a. Has the Website coordinator / Web-content manager established information-product inventories and schedules for archiving / updating those products?				OMB M-05-04; OMB Circular A-130; Paperwork Reduction Act; E-government Act.
9b. Has the coordinator / manager submitted an E-Gov Act report on inventories, priorities, and schedules?				
10. Has the Website established, and does it maintain, communication (such as user surveys or questionnaires) with members of the public to ensure that it offers information products meeting the public's needs?				OMB M-05-04; CFR Section 1320.
11. Does the Website offer assistance to the public in locating government information, such as a search function, sitemap, or subject index?				OMB M-05-04; DA PAM 25-1-1.
12. Is the Website on an approved domain?				OMB M-05-04; DoDI 8410.1; Paragraph 6-7b, AR 25-1.
13. Has the Website implemented adequate security controls?				OMB M-05-04. Minimum federal standards are in OMB Circular A-130, Appendix III; OMB memo M-04-25; NIST

				Special Pub 800-44; and other associated guidance from NIST. Adequate security controls must be in place to ensure that information is resistant to tampering to preserve accuracy; remains confidential as necessary; and the information or service is available. Minimum Army standards are in AR 25-2.
14a. Is the installation telephone directory on AKO?				Paragraph 6-4r, AR 25-1.
14b. Are any organizational collaboration / coordination sites on AKO?				Paragraph 6-7a(15), AR 25-1.
15. Has the Website implemented features that will make processing FOIA requests more streamlined and effective, as well as increasing the public's reliance on using the Website to retrieve records without requiring them to request records under the FOIA?				Section 3(b)(ii), EO 13392.
16. Does the organization have a COOP plan for its Website?				Paragraph 8-1c(4)(a), DA PAM 25-1-1.
Corporate ethos / corporate branding				
17. Has the Website adopted the principles of "strategic Webbing"?				Answers to Qs 18a through 19f must be "Yes" before the answer to Q17 can be "Yes."
Corporate cohesion: 18. Does the Website conform to the principle of corporate cohesion?				IAW Paragraph 8-1i, DA PAM 25-1-1.
18a. Is the phrase "U.S. Army" clearly displayed on every Webpage, along with the organization's official name?				Answers to Qs 18a through 18h must be "Yes" before the answer to Q18 can be "Yes."
18b. Does the Website contain the statement "This Website contains official government information"?				
18c. Does the page title on the homepage and major pages linked from the homepage include the organization's name identified as the site sponsor?				
18d. Do all HQ TRADOC organizational homepages follow the template provided by the TRADOC G-6?				
18e. Do the TRADOC homepage and pages linked off the TRADOC homepage include the command's major communication themes?				IAW TR 25-1.
18f. Do command / activity homepages incorporate TRADOC and local communication themes into Website displays?				
18g. Does each Webpage link back to the Website's homepage and to its parent organization's homepage?				IAW TR 25-1.
18h. Do all TRADOC sites link to:				IAW TR 25-1.
--The next senior Website in the hierarchy IAW TR 10-5;				
--The organizational homepage on AKO if one exists;				
--The TRADOC logo and motto;				
--The HQ TRADOC homepage; and				
--The Army homepage (www.army.mil)				

Corporate identity ("brand"): 19. Does the Website conform to the principle of corporate identity / branding?				Answers to Qs 19a through 19f must be "Yes" before the answer to Q19 can be "Yes."
19a. Does the Webpage design for commands / activities make it distinguishable – "branded," with a unique design, corporate identity, and clear demarcation – from garrison or other tenant activities at their installations?				
19b. Does each Website have a clearly defined purpose statement and Website plan that states the organization's mission, outlines its structure, and is approved by the organization's parent command or organization?				
19c. Does the organization mission / structure content include site registration?				
19d. Does the organization mission / structure content include mission Webmaster / portal administrator contact information?				
19e. Does the organization mission / structure content include procedures that explain posting of information and review of the site for content and format?				
19f. Does the organization mission / structure content include an explanation of contingency and COOP plans, describing what the organization will do with its Website during disasters or emergencies, and what important information and services will be provided to the public?				
20. Have official entries on social-media sites been reviewed by both OPSEC and PAO before release?				

Chapter 5

Recordkeeping and file management

Army regulations require that information used in decision-making and Army business processes be considered *Army record material*, whether stored electronically or as a hard copy. Army record material is created, scheduled, maintained, preserved, and disposed of IAW AR 25-400-2.⁵⁶⁸ Maintaining Army information that meets the definition of a record is the responsibility of all military, civilian, and contractor personnel, commanders, and leaders, but personnel are required to create only the minimum records essential and adequate to support, sustain, and document 1) military operations in time of peace, war, and operations-other-than-war (for example, contingency operations and humanitarian, peacekeeping, and nation-building missions), or regarding 2) the conduct of all other activities of the Army's official business.⁵⁶⁹ Recordkeeping requirements are found in Paragraph 5-4, TR 25-1; Section II of Appendix F, AR 380-5; Chapter 8, AR 25-1; and Chapters 5, 6, and 7 in AR 25-400-2⁵⁷⁰; among other sources. This *Guide* discusses them only inasmuch as Web content becomes short- and long-term official records.

As part of documenting Army business processes, organizations with public Websites must keep records of content reviews, IAW DA PAM 25-1-1, Paragraph 7-7j, as well as AR 380-5, Paragraphs 1-13 and 4-15b. G-6 and PAO may also keep written records of violation notifications. All organizations must manage Web records per OMB Circular A-130 and guidance from NARA (see 36 CFR 1220-1238 and www.archives.gov/records_management/index.html).⁵⁷¹

The point of records management is to capture, preserve, and make available evidence essential for Army decisions and actions; meet the needs of the American public; and protect the rights and interests of the government and individuals.⁵⁷² Required by the Federal Records Act (44 USC Chapter 31),⁵⁷³ federal-government records are “made or received by any DA entity under federal law or in connection with the transaction of public business and preserved – or are appropriate for preservation by DA as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of DA or because of the informational value of the data in them.”⁵⁷⁴ Therefore TRADOC Webpages may be considered official command records if they document the mission and current organizational structure of TRADOC, as well as key functions, policies, decisions, procedures, or operations. (See a following section titled “Electronic-records management” for more information on what a record is and isn’t.)

Files on AKO / DKO that are determined to be records will also be managed per Chapter 8, AR 25-1, and AR 25-400-2.⁵⁷⁵

Consult Army records-management officials such as G-6 for the requirements and procedures in determining and preserving Web-content as records, since “the conduct of all other activities of the Army’s official business” is a broad category.⁵⁷⁶ The records-management hierarchy begins with the AASA, who serves as archivist of the Army and the senior Army official for records management and associated programs (specified in Paragraph 8-5, AR 25-1).⁵⁷⁷ The AASA is responsible for the executive coordination and interface with the U.S. archivist, promoting cooperation with the U.S. archivist in applying standards, procedures, techniques, and schedules designed to improve records management, safeguard maintenance and security of records determined as appropriate for preservation, and facilitate segregation and disposal of temporary-value records.

As the Army archivist may delegate responsibilities for achieving the records-management mission, the AASA has delegated some of the mission to the AASA’s Records Management and Declassification Agency (RMDA). RMDA is “responsible for the entire spectrum of Army-wide interrelated records-management programs and associated functional automation systems which have significant interest” from the Executive Branch, Congress, DoD / Army

⁵⁶⁸ Paragraph 1-6e, AR 25-1.

⁵⁶⁹ Paragraph 8-3a, AR 25-1.

⁵⁷⁰ See Paragraph 1-13, AR 380-5, for example.

⁵⁷¹ Paragraph 8-1g, DA PAM 25-1-1.

⁵⁷² Paragraph 8-1, AR 25-1.

⁵⁷³ Paragraph 8-2a, AR 25-1.

⁵⁷⁴ Paragraph 8-2c, AR 25-1.

⁵⁷⁵ Paragraph 6-7d(8), AR 25-1.

⁵⁷⁶ An introductory note on Chapter 8, AR 25-1, explains that IAW DA General Order 2006-01, the Army’s records-management function transferred from the Army DCS G-1, to the AASA. “Performance of the missions and functions” continues under the CIO / G’6’s oversight.

⁵⁷⁷ Paragraphs 2-8a and 2-8b, AR 25-1.

leadership, Soldiers, veterans, and the public.⁵⁷⁸ Declassification, Army FOIA, Army Privacy Act, QI, and Joint-records research all fall under RMDA. RMDA is the only activity authorized to schedule records disposition with NARA,⁵⁷⁹ and therefore the RMDA's director takes final action to offer records to NARA.⁵⁸⁰ Consult RMDA's Website and possibly contact RMDA regarding Web-records requirements.

At minimum, RMDA's objectives are to cost-effectively organize Army records stored on any medium (including Web records) so needed records can be found rapidly; ensure that records are complete, accurate, authentic, reliable, and trustworthy; facilitate the selection and retention of records of enduring value; and accomplish the prompt disposition of unscheduled records in accordance with NARA-approved disposition schedules.⁵⁸¹ Organizations' maintenance and disposition of Web records should be IAW those objectives.

WEB FILES MANAGEMENT

Once files are posted on the Web, the organization's Webmaster or the content provider is responsible for deleting files no longer needed on any drive space used for the content-review process. The organization's Webmaster or the content provider should keep a copy of all documents as a backup if appropriate. PAO and G-6 may keep copies of files, but Webmasters and content providers should not rely on this – backup copies are the organization's responsibility.

Each organizational Website coordinator should develop a method for managing volume, controlling versions, ensuring approvals by all appropriate authorities (in coordination with content providers), and controlling movement from the organization's file directories to the TRADOC Webserver (in coordination with the organization's Webmaster). Website coordinators in coordination with Webmasters should also consider, based on the content of their organizational Webpages, how many versions to track, how long to keep them, and where they are physically stored. A specific method is not mandated, but Website coordinators may find that even for a small number of Webpages, they will need some method of management control.

The Webpage residing on the TRADOC Webserver is the primary file. No files – e.g., backups and old files – other than the primary file should reside on the TRADOC external Webserver. The TRADOC Webmaster may remove files from the external Webserver if the organizational Webmaster or Website coordinator cannot fulfill his / her responsibility for recordkeeping and file management.

For continuity, which enhances recordkeeping and file management, TRADOC PAO recommends that each organization have some method to ensure that all potential Webpage authors have proper Web-content training and access to this *Guide*. The organization's Webmaster should have a backup Webmaster, and all Web-related correspondence should include both of them.

Webmasters must also periodically review their pages. DA mandates a review every quarter.

ELECTRONIC-RECORDS MANAGEMENT

As federal records, TRADOC Webpages are subject to the retention and disposition rules authorized by NARA, since electronic records appraised as permanent records may be transferred to NARA. (See Chapter 8, AR 25-1.)

IAW Paragraph 8-2c, AR 25-1, federal records include the following Web-related formats:

- All documents, maps, photographs, and graphic art.
- Record information stored on machine-readable media. These include all electronic formats (office automation software – for example, word processing, spreadsheet, presentations), email, Websites, ISs, databases, and printouts.
- Audio and video recordings (see DoDI 5040.6 and Chapter 7 of AR 25-1).
- Any other documentary materials regardless of physical form or characteristics.

IAW Paragraph 8-2d, AR 25-1, the following Web-related objects are not included in the statutory definition of the word *record* (also see DoDI 5400.7-R and AR 25-55):

⁵⁷⁸ From Website, <https://www.rmda.army.mil>.

⁵⁷⁹ Paragraph 8-5a, AR 25-1.

⁵⁸⁰ Paragraph 8-5n, AR 25-1.

⁵⁸¹ Paragraph 8-5a, AR 25-1.

- Extra copies of documents preserved only for convenience or reference. Copies of such materials should be kept to a minimum.
- Commercially exploitable resources, including but not limited to:
 - Maps, charts, map compilation manuscripts, map research materials, and data, if not created or used as primary sources of information about organizations, policies, functions, decisions, or procedures of DA.
 - Computer software, if not created or used as primary sources of information about organizations, policies, functions, decisions, or procedures of DA. This does not include the underlying data processed and produced by such software, which may in some instances be stored with the software.
- Unaltered publications and processed documents – such as regulations, manuals, maps, charts, and related geographical materials – which are available to the public through an established distribution system, with or without charges.
- Information stored within a computer for which there is no existing computer software program to extract the information or a printout of the information.

In addition to the current version of a Webpage, previous versions may also qualify as official records. See NARA guidance at <http://www.archives.gov/records-mgmt/initiatives/web-content-records.html> for information on determining which Web-content records are permanent and when transfer of permanent, official records to NARA should occur. Previous versions of a Webpage that do not qualify as official records are defined as *non-record material* and should be overwritten or deleted from the Webserver within seven working days of the final posting of the Webpage's updated version.

Requests for waivers or exceptions should be submitted to TRADOC G-6 Records Management. Neither record (previous versions) nor non-record documents should reside on the external Webserver.

Chapter 6

Required and recommended training

According to the DoD IG's audit report of the TRADOC Web Content Review Program, mentioned in an earlier chapter, "[t]raining ... is a first step to safeguarding sensitive information."⁵⁸² The concerns about safeguarding have been the major driver behind the requirements for "Web OPSEC training" mandated by DoD senior leadership. This chapter discusses the requirements and our recommendations.

MANDATORY WEB TRAINING

Webmasters / portal administrators, PAO content reviewers, other content reviewers, and Web-content providers first became required to complete training and certification IAW ALDODACT message 11/06, published in August 2006. Mandated jointly by the DEPSECDEF and Vice Chairman of the Joint Chiefs of Staff (VCJCS), all command OPSEC managers and Webmasters who review information for public release on DoD Websites must have Web OPSEC training. Public Affairs specialists who review information for Web posting must also receive Web OPSEC training. Not mandatory, but encouraged, is OPSEC training for Webmasters who work directly with Website management or supervision.⁵⁸³

ALDODACT 11/06 did not specify any training courses but recommended two courses that the Interagency OPSEC Support Staff (IOSS) sponsors. ALDODACT 11/06 also said that other Web-specific OPSEC training may be available locally that fulfills the requirement.

About two years later (September 2008), the DEPSECDEF issued another memo, "Department of Defense (DoD) Website Security Policy Compliance," requiring DoD components to certify two things: 1) that they had implemented a review-and-approval process for all information posted to publicly accessible Websites, and 2) that personnel responsible for reviewing information had received mandatory Web OPSEC training. The DEPSECDEF's memo reiterated the training requirements of ALDODACT 11/06 for PAOs, Webmasters / maintainers, and OPSEC / IA specialists: "On Aug. 6, 2006, the [VCJCS] and I issued a joint message, "Information Security / Web Site Alert" [ALDODACT 11/06] to the components requesting they ensure information placed on publicly accessible Websites is [IAW] security requirements in [DoD's] 'Website Administration Policies and Procedures' ... and is reviewed for security concerns by personnel trained in [OPSEC]. ... The lack of adherence to the Web-security policy has been brought to the attention of the [IG], requesting that he include this matter as one of particular interest in executing his oversight responsibility."

Senior leadership believes that training is critical to ensuring sensitive information is identified, properly controlled, and not accidentally posted to public Websites. In fact, the Office of the Army IG, as part of its IA inspection mission, will inspect to validate that Web content and OPSEC training certification is completed, in addition to the current inspections it performs on command Websites for OPSEC.⁵⁸⁴

After the DEPSECDEF's September memo, an Army message issued in December 2008 not only tasked Army organizations to certify that they had a review program, but required mandatory Web-content and OPSEC training for Web-content reviewers via a Web-based application. The mandatory course, "Web Content and OPSEC Certification Training," can be accessed at <https://iatraining.us.army.mil/index.php>.

This course contains four modules: Web content and OPSEC introduction module, DoD Webmaster module, Web-content module, and OPSEC module. Certificates are issued after the student passes the final test. The Army message requires that the student's certificate be presented to his / her leadership after the student completes training: "Individuals must provide proof they completed the training to their respective organizations. Certificates dated from [Jan. 1, 2008] to the present may be used as proof of training."⁵⁸⁵

TRADOC PAO recommends that all individuals appointed as Webmasters / portal administrators, content providers, content reviewers, or Website coordinators / Web-content managers complete Army training and certification.⁵⁸⁶

⁵⁸² Page 10, DoD Office of the IG, "Army Website Administration, Policies and Practices (D-2002-098)," June 5, 2002.

⁵⁸³ Paragraph 7, ALDODACT message 11/06. Also see the SECDEF message, "Website OPSEC Discrepancies" (ALDODACT 02/03), Jan. 14, 2003, and Paragraph 5b(5), TRADOC OPSEC Plan.

⁵⁸⁴ Paragraph 4C, ALARACT, "Website Security Policy Compliance," Dec. 19, 2008.

⁵⁸⁵ Paragraph 4B, ALARACT, "Website Security Policy Compliance," Dec. 19, 2008.

⁵⁸⁶ See Paragraph 8-4b, DA PAM 25-1-1; Paragraph 5-5a(5), TR 25-1.

These individuals should review the modules regularly to maintain familiarity with the material. We highly recommend that refresher training be completed annually.

A separate Army message – issued from Army G-3/5/7 previous (in March 2008) to the DEPSECDEF’s memo and the Army’s corresponding message – required **all Army personnel** (Soldiers, DA civilians, and contractors) to **review an unclassified IA briefing** at <https://ia.gordon.army.mil/dodiaa/default.asp>. (Family members access the IA training at http://iase.disa.mil/eta/iaa-trainingv6/dod_iaa_v6/index.html.) This training, which meets the Army’s requirement for an annual IA-compliance-training update, is a separate requirement from the Web-content OPSEC training, although there may be some subject overlap.⁵⁸⁷

ELECTIVE / RECOMMENDED OPSEC TRAINING

Not mandatory but appropriate in meeting the DEPSECDEF’s / VCJCS’s Web-training requirement are IOSS’ “OPSEC and Web Risk Assessment” (OPSE-3500) and “OPSEC and Public Release Decisions” (OPSE-1500). OPSE-3500 is a resident course taken at IOSS’ facility in Greenbelt, Md. OPSE-1500, which is recommended especially for Public Affairs personnel, is taught there as well but is also available through IOSS’ e-learning program; see <http://www.ioiss.gov/calendar.html> for IOSS’ training calendar and <http://www.ioiss.gov/training/1500.html> for more details on the course.

Elective OPSEC training may be accomplished through the 1st Information Operations Command (IOC) Website at <https://OPSEC.1stiocmd.army.mil> – see the “Other Training” tab for a listing.

Personnel who are required to accomplish Web-content review may also request the three-day HQ DA OPSEC Officer Certification Course. In fact, OPSEC officer training and certification (Level II) is mandatory for those who will be accomplishing OPSEC review of material proposed for the public domain – including proposed Web content prior to dissemination of the information.⁵⁸⁸ Attendance at the HQ DA OPSEC officer or DA-approved OPSEC Mobile Training Team (MTT) courses may be requested through 1st IOC. Level II certification may also be achieved through IOSS’ OPSE-2400 resident course (or via MTT if there are 25 students at one location).

Either OPSE-1300 or OPSE-1301 (computer-based training via a CD that can be viewed on your desktop), or other equivalent fundamentals course, is a prerequisite to attend OPSE-2400. OPSE-1301 can be ordered from IOSS. OPSE-1300 is available via platform instruction or MTT.

For more information, see <http://www.ioiss.gov/>. See <http://www.ioiss.gov/calendar.html> for a training calendar.

PUBLIC AFFAIRS PROFESSIONAL TRAINING

Although Web and OPSEC training may be attained in DoD and Army Public Affairs schools, at this time a specific course is mandated to fulfill Web OPSEC training requirements, as stated above. DoD and Army Public Affairs training focuses more on:

- Engaging the public, including target populations in regional operations areas, via diverse newsmedia outlets.⁵⁸⁹
- Successfully planning, integrating, executing, and evaluating Public Affairs operations.⁵⁹⁰
- Providing Public Affairs training for non-Public Affairs personnel at military service schools to enhance DoD’s capability to research, plan, execute, and assess communications strategies, foster media relations, and improve internal communications across DoD.⁵⁹¹

Public Affairs training is conducted at Defense Information School (DINFOS) and through simulation / exercise and education programs.

⁵⁸⁷ ALARACT 089/2008 issued by Army DCS G-3/5/7, “Securing AKO Content and Credentials (NIPR),” March 25, 2008.

⁵⁸⁸ Email from TRADOC OPSEC officer dated April 9, 2009: “DA requires that the person reviewing OPSEC be Level II trained.”

⁵⁸⁹ Paragraph 5c, Enclosure 2, DoDI 5400.13.

⁵⁹⁰ Paragraph 5d, Enclosure 2, DoDI 5400.13.

⁵⁹¹ Paragraph 7c, Enclosure 2, DoDI 5400.13.

IT / IA PROFESSIONAL TRAINING

DoD's policy is that a well-trained core of highly qualified IRM / IT and IA professionals be developed who can accept, anticipate, and generate the changes that the DDIE's evolution will cause in DoD's net-centric operations. Similarly, the entire DoD workforce is expected to be trained and ready to "take advantage" of the DDIE.⁵⁹² Therefore we do not anticipate any lessening of DoD's mandatory IT and IA training requirements.

Some of the regulatory requirements are:

- All Army personnel appointed as IA or network-operations personnel must successfully complete an IA security training certification course of instruction equivalent to the duties assigned to them. Individuals must also be certified IAW the DoD baseline requirements of DoD 8570.1M,⁵⁹³ **IA Training, Certification and Workforce Management**.⁵⁹⁴
- All positions in which personnel have or require access to an IT system will be designated as an IT position IAW AR 25-2. As stated, individuals must complete training and certification, as necessary, equal to their assigned duties.⁵⁹⁵

AR 25-1 requires Army organizations to provide their Webmasters / maintainers sufficient resources and training on both technical and content matters. Resources are available on the Army Webmaster's homepage, <http://www.army.mil/webmasters/>.⁵⁹⁶

On-line training is also available at https://iatraining.us.army.mil/_usermgmt/login.htm and http://www.disa.mil/handbook/handbook_v1.6.doc.⁵⁹⁷

OTHER OPSEC RECOMMENDATIONS

Personnel should be very familiar with the TRADOC Essential Elements of Friendly Information (EEFI) and the TRADOC OPSEC Plan in general when accomplishing content reviews. HQ TRADOC PAO personnel must comply with the **TRADOC OCPA OPSEC SOP** when performing content reviews.

⁵⁹² Paragraph 4j, DoDD 8000.01.

⁵⁹³ Paragraph 4-3, AR 25-2.

⁵⁹⁴ Joint message from the commander of U.S. Strategic Command and ASD-NII, "Support for Information Assurance and Computer Network Defense (CND) Assessments, Priorities, Initiatives and Processes," April 7, 2004; Paragraph 5.7, Part II, DoD Web policy.

⁵⁹⁵ Paragraphs 5-7a and 5-7b, AR 25-1.

⁵⁹⁶ Paragraph 6-7a(13)(a), AR 25-1.

⁵⁹⁷ Paragraph 6-7a(13)(b), AR 25-1.

Summary

Throughout this user guide, it should be evident that many policies affect Web content, and managing it is best served by a team. Several teams, in fact: the team that safeguards information (OPSEC, G-6, and PAO); the team that creates and manages content (content provider, content reviewer, and Website coordinator / Web-content manager) to ensure it is accurate, relevant, and timely; and the WCWG, which serves as the guiding coalition to treat Websites as a core business function.

But the person in the catbird seat is the Web-content manager, the person who 1) is able to view Web content holistically; 2) understands the Website target audience's information needs; 3) is detail-oriented enough to ensure an efficient, robust Web-content review process is established within the organization; and 4) is strategist enough to plan and evaluate the organization's Web content for improvement to ensure a lively, relevant Web presence. The one who actually makes or breaks the Website is the Web-content manager.

This is important because an organization's public Website is a vital communication venue. The WWW provides the Army with a powerful tool to convey information quickly and efficiently on a broad range of topics relating to its activities, objectives, policies, programs, and personnel. The global reach of the Web makes this information easily accessible to the men and women of the armed forces, their families, the American public, and the international audience. It is practically an *obligation* to use the Web and social media to communicate the importance of what TRADOC is doing for the Army and the nation – especially with all the bad-news stories circulating that make the Army appear “broke.”

What we have to be careful of is that information on publicly accessible Websites and in social media often provides too much detail on DoD capabilities, infrastructure, personnel, and operational procedures – past, present, and future. While it may be true that most of this information is wholly, and truly, unclassified, when combined with information from other sources and / or sites, the information can become sensitive and even classified. The information also may increase the vulnerability of DoD systems and may potentially be used to threaten or harass DoD personnel and / or their families.⁵⁹⁸ Maintaining public Websites and engaging in social media is actually an awesome responsibility, if you think about it.

“The boss” must be involved in the organization's Web presence. All commanders / leaders who establish publicly accessible Websites are responsible for ensuring that the information published on their sites does not compromise national security or place DA personnel at risk. The commander's / leader's responsibility extends beyond general Public Affairs considerations about releasing information into the realm of OPSEC and force protection.⁵⁹⁹ Commanders / leaders must apply comprehensive risk-management procedures to ensure that the considerable mission benefits gained by using the Web and social media are carefully balanced against the potential security and privacy risks created by having aggregated DoD information more readily accessible to a worldwide audience than ever before.⁶⁰⁰

But the vitality of Web content ultimately rests at the feet of all DoD personnel, who should also have a heightened security awareness concerning their day-to-day duties and recognize that the nation's increased security posture will remain a fact of life indefinitely.⁶⁰¹

⁵⁹⁸ Paragraph E-1b, Appendix E, AR 380-5.

⁵⁹⁹ Memorandum from DEPSECDEF, “Information Vulnerability and the Worldwide Web,” Sept. 24, 1998; Paragraph E-1b, Appendix E, AR 380-5.

⁶⁰⁰ Paragraph E-1b, Appendix E, AR 380-5.

⁶⁰¹ Memorandum from OSD, “Withholding of Personally Identifying Information Under the Freedom of Information Act (FOIA),” Nov. 9, 2001.

Appendix A References

References are organized by topic, then listed with the latest reference published first, in reverse order to earliest published reference. This is done because later references at times affect parts of the policy in earlier references while not superseding the publication; when using earlier references, always check the later ones for “amplification” to policy and guidance. Links to DoD / Army information portals are also provided.

CLEARANCE / RELEASE OF INFORMATION (ALSO SEE POLICY AND GUIDANCE, WEB)

Department of Defense Instruction 5230.29, *Security and Policy Review of DoD Information for Public Release*, Jan. 8, 2009, <http://www.dtic.mil/whs/directives/corres/pdf/523029p.pdf>.

Department of Defense Instruction 5400.13, *Public Affairs (PA) Operations*, Oct. 15, 2008, <http://www.dtic.mil/whs/directives/corres/pdf/540013p.pdf>.

Department of Defense Directive 5122.05, *Assistant Secretary of Defense for Public Affairs (ASD(PA))*, Sept. 5, 2008, <http://www.dtic.mil/whs/directives/corres/pdf/512205p.pdf>.

Department of Defense Directive 5230.9, *Clearance of DoD Information for Public Release*, Aug. 22, 2008, <http://www.dtic.mil/whs/directives/corres/pdf/523009p.pdf>.

Memorandum from Chief of Army Public Affairs, “Required Public Affairs Review of Information Released Publicly via Army Headquarters Websites,” April 28, 2003.

Department of Defense Directive 5410.18, *Public Affairs Community Relations Policy*, Nov. 20, 2001, <http://www.dtic.mil/whs/directives/corres/pdf/541018p.pdf>.

Field Manual 3.61.1, *Public Affairs Tactics, Techniques and Procedures*, October 2000, https://rdl.train.army.mil/soldierPortal/atia/adlsc/view/public/11644-1/fm/3-61.1/fm3_61x1.pdf.

Army Regulation 360-1, *The Army Public Affairs Program*, Sept. 15, 2000 [currently being updated], http://www.apd.army.mil/jw2/xmldemo/r360_1/cover.asp or http://www.apd.army.mil/pdffiles/r360_1.pdf.

FREEDOM OF INFORMATION ACT (FOIA) (ALSO SEE PII REFERENCES)

Memorandum from U.S. Attorney General, “The Freedom of Information Act (FOIA),” March 19, 2009.

Memorandum from President Barack Obama, “Transparency and Open Government,” Jan. 21, 2009, http://www.whitehouse.gov/the_press_office/Transparency_and_Open_Government.

Memorandum from President Barack Obama, “Freedom of Information Act,” Jan. 21, 2009, http://www.whitehouse.gov/the_press_office/Freedom_of_Information_Act.

Joint memo from the director of the Army Staff and the administrative assistant to the Secretary of the Army, “Freedom of Information Act (FOIA) Program,” Sept. 17, 2008.

Department of Defense Directive 5400.07, *DoD Freedom of Information Act (FOIA) Program*, Jan. 2, 2008, <http://www.dtic.mil/whs/directives/corres/pdf/540007p.pdf>.

DoD publication 5400.7-R, *Department of Defense Freedom of Information Act Program*, Sept. 4, 1998, and Change 1 April 11, 2006, <http://www.dtic.mil/whs/directives/corres/pdf/540007r.pdf>.

32 Code of Federal Regulations, Part 518, Freedom of Information Act Program, final rule (published in *Federal Register* to update Army FOIA program), Feb. 22, 2006, <https://www.rmda.army.mil/foia/docs/foia-32CFRPart518.pdf>.

Executive Order 13392, *Improving Agency Disclosure of Information*, Dec. 14, 2005, <http://edocket.access.gpo.gov/2005/pdf/05-24255.pdf>.

Memorandum from the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD-C3I), “Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites,” Dec. 28, 2001, http://www.defenselink.mil/pubs/foi/names_removal.pdf.

Memorandum from the Directorate for Freedom of Information and Security Review (DFOISR), “DoD Guidance on Attorney General Freedom of Information (FOIA) Memorandum,” Nov. 19, 2001, <http://www.dod.mil/pubs/foi/AGmemo.pdf>.

Memorandum from the Director of Administration and Management, Office of the Secretary of Defense (OSD), “Withholding of Personally Identifying Information Under the Freedom of Information Act (FOIA),” Nov. 9, 2001, <http://www.defenselink.mil/pubs/foi/withhold.pdf>.

Army Regulation 25-55, *The Department of the Army Freedom of Information Act*, Nov. 1, 1997, http://www.apd.army.mil/pdffiles/r25_55.pdf or http://www.apd.army.mil/jw2/xmldemo/r25_55/cover.asp.

RMDA FOIA Webpage, <https://www.rmda.army.mil/programs/foia.shtml>.

Department of Defense service center for FOIA requests, <http://www.dod.mil/pubs/foi/>.

INFORMATION QUALITY

Office of Management and Budget (OMB) memorandum M-05-04, “Policies for Federal Agency Public Websites,” Dec. 17, 2004, <http://www.whitehouse.gov/omb/memoranda/fy2005/m05-04.pdf>.

Headquarters Department of the Army Letter 25-03-02, “Ensuring Quality of Information Disseminated to the Public by the Department of Defense,” Oct. 28, 2003, http://www.apd.army.mil/pdffiles/l25_03_2.pdf; expired Oct. 28, 2005; included now in Army Regulation 25-1 and Department of the Army Pamphlet 25-1-1.

Memorandum from the Deputy Secretary of Defense, “Ensuring Quality of Information Disseminated to the Public by the Department of Defense,” Feb. 10, 2003, in DoD publications archives at http://www.defenselink.mil/pubs/016_DEPSECDEFInfoQualMemo.html. Also included as attachments to HQ DA Letter 25-03-02, http://www.apd.army.mil/pdffiles/l25_03_2.pdf.

Office of Management and Budget (OMB) memorandum, “Executive Branch implementation of the Information Quality Law,” Oct. 4, 2002, http://whitehouse.gov/omb/inforeg/pmc_graham_100402.pdf.

DoD information quality Website, <http://www.defenselink.mil/pubs/dodiqguidelines.html>.

MISCELLANEOUS

Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, April 12, 2001 (as amended through March 17, 2009), http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf.

Army Regulation 5-22, *The Army Force Modernization Proponent System*, Feb. 6, 2009, http://www.apd.army.mil/jw2/xmldemo/r5_22/cover.asp or http://www.apd.army.mil/pdffiles/r5_22.pdf.

Army Regulation 600-20, *Army Command Policy*, rapid-action revision dated Feb. 11, 2009, on regulation version of March 18, 2008, http://www.apd.army.mil/jw2/xmldemo/r600_20/cover.asp or http://www.apd.army.mil/pdffiles/r600_20.pdf.

Department of Defense Inspector General report, *Organizational Structure and Managers’ Internal Control Program for the Assistant Secretary of Defense (Public Affairs) and American Forces Information Service*, (D-2009-028), Dec. 10, 2008, <http://www.dodig.mil/Audit/reports/fy09/09-028.pdf>.

Putting Citizens First: Transforming On-line Government, Federal Web Managers Council, whitepaper written for the Presidential Transition Team, November 2008, http://www.usa.gov/webcontent/documents/Federal_Web_Managers_WhitePaper.pdf.

TRADOC Regulation 1-8, *TRADOC Operations Reporting*, rapid-action revision of Jan. 31, 2008, <http://www.tradoc.army.mil/tpubs/regs/r1-8.pdf>.

Department of Defense Directive 5500.07, *Standards of Conduct*, Nov. 29, 2007, <http://www.dtic.mil/whs/directives/corres/pdf/550007p.pdf>.

Department of Defense Instruction 5040.5, *Alteration of Official DoD Imagery*, June 6, 2006, <http://www.dtic.mil/whs/directives/corres/pdf/504005p.pdf>.

Joint Ethics Regulation (JER), DoD 5500.7-R, Aug. 1, 1993, with latest change (Change 6) dated March 23, 2006, http://www.doc.mil/dodgc/defense_ethics/ethics_regulation.

Memorandum from the Deputy Secretary of Defense, “2006 Quadrennial Defense Review (QDR) Strategic Communication (SC) Execution Roadmap,” Feb. 6, 2006.

Army Regulation 215-1, *Morale, Welfare and Recreation Activities and Nonappropriated Fund Instrumentalities*, Sept. 15, 2005, http://www.apd.army.mil/pdffiles/r215_1.pdf.

Army Regulation 380-10, *Foreign Disclosure and Contacts with Foreign Representatives*, June 22, 2005, http://www.apd.army.mil/jw2/xmldemo/r380_10/cover.asp or http://www.apd.army.mil/pdffiles/r380_10.pdf.

Memorandum from Assistant Secretary of Defense for Public Affairs (ASD-PA), “Visual Information (VI) Activity Management,” March 25, 2004.

Army Regulation 5-1, *Total Army Quality Management*, March 15, 2002, http://www.apd.army.mil/jw2/xmldemo/r5_1/cover.asp or http://www.apd.army.mil/pdffiles/r5_1.pdf.

Strategic Communications for Nonprofit Organizations, Janel Radtke, John Wiley & Sons, 1998.

Department of Defense Instruction 5120.4, *Department of Defense Newspapers, Magazines and Civilian Enterprise Publications*, June 16, 1997, <http://www.dtic.mil/whs/directives/corres/pdf/512004p.pdf>.

The Handbook of Strategic Public Relations & Integrated Communications, Clarke L. Caywood (editor), McGraw Hill Books, 1997.

Army Web Content and OPSEC Module on-line training (OPSEC-Web-4100), <https://iatraining.us.army.mil>, undated.

Web Content and OPSEC Certification Training, DoD Web Guidance Training Module (Web-DoD-001), <https://iatraining.us.army.mil>, undated.

Department of the Army Pamphlet 25-91, *Visual Information Procedures*, Sept. 30, 1991, http://www.apd.army.mil/jw2/xmldemo/p25_91/cover.asp.

Department of Defense issuances and instructions portal, <http://www.dtic.mil/whs/directives/index.html>.

POLICY AND GUIDANCE, WEB

TRADOC memorandum, “TRADOC Public Website Content Management,” June 11, 2009.

Department of Defense Directive 8000.01, *Management of the Department of Defense Information Enterprise*, Feb. 10, 2009, <http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf>.

Army Regulation 25-1, *Army Knowledge Management and Information Technology Management*, Dec. 4, 2008, http://www.apd.army.mil/pdffiles/r25_1.pdf.

Department of Defense Website administration policy and procedures, Nov. 25, 1998, with amendments and corrections May 9, 2008, <http://www.defenselink.mil/cio-nii/policy/WebSiteAdminGuidance.pdf>.

Department of Defense Instruction 8410.01, *Internet Domain Name Use and Approval*, April 14, 2008, <http://www.dtic.mil/whs/directives/corres/pdf/841001p.pdf>.

TRADOC Regulation 25-1, *Information Resources Management*, Sept. 16, 2006 [currently being updated], <http://www.tradoc.army.mil/tpubs/regs/r25-1.pdf> or <http://www.tradoc.army.mil/tpubs/regs/r25-1.doc>.

All DoD activities (ALDODACT) message 11/06 (joint message from Deputy Secretary of Defense / Vice Chairman of the Joint Chiefs of Staff), “Information Security / Website Alert,” Aug. 9, 2006, <http://www.defenselink.mil/webmasters/policy/infosec20060806.html>.

Department of the Army Pamphlet 25-1-1, *Information Technology Support and Services*, March 20, 2006, http://www.apd.army.mil/jw2/xmldemo/p25_1_1/cover.asp or http://www.apd.army.mil/pdffiles/p25_1_1.pdf.

Office of Management and Budget (OMB) memorandum M-05-04, “Policies for Federal Agency Public Websites,” Dec. 17, 2004, <http://www.whitehouse.gov/omb/memoranda/fy2005/m05-04.pdf>.

Message from the Secretary of Defense, “Website OPSEC Discrepancies” (ALDODACT 02/03), Jan. 14, 2003, http://www.defenselink.mil/webmasters/policy/rumsfeld_memo_to_DOD_webmasters.html.

Department of Defense Inspector General report on Army Website management (D-2002-098), includes TRADOC Website management, June 5, 2002, <http://www.dodig.mil/Audit/reports/fy02/02-098.pdf>.

Memorandum from the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD-C3I), "Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites," Dec. 28, 2001, http://www.defenselink.mil/pubs/foi/names_removal.pdf.

Army Regulation 360-1, *The Army Public Affairs Program*, Sept. 15, 2000 [currently being updated], http://www.apd.army.mil/pdffiles/r360_1.pdf or http://www.apd.army.mil/jw2/xmldemo/r360_1/cover.asp.

Memorandum from the Deputy Secretary of Defense, "Information Vulnerability and the Worldwide Web," Sept. 24, 1998, http://www.defenselink.mil/other_info/depsecweb.pdf.

Army Webmaster policy portal, <http://www.army.mil/ciog6/references/webmaster/policy.html>.

Defense Department Webmaster policy portal, <http://www.defenselink.mil/webmasters/>.

PRIVACY / PERSONAL INFORMATION (ALSO SEE FOIA REFERENCES)

All Army activities (ALARACT) message 050/2009, "Personally Identifiable Information (PII) Incident Reporting and Notification Procedures," Feb. 26, 2009, https://www.rmda.army.mil/privacy/docs/ALARACT_050_2009_1.pdf.

Office of Management and Budget (OMB) document M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifying Information," May 22, 2007, <http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf>.

Department of Defense Directive 5400.11, *DoD Privacy Program*, May 8, 2007, <http://www.dtic.mil/whs/directives/corres/pdf/540011p.pdf>.

Part 505, 32 Code of Federal Regulations, *The Army Privacy Program*, Sept. 11, 2006.

All Army activities (ALARACT) message 138/2006, "DoD Personnel Responsibility for Safeguarding Personally Identifiable Information," May 26, 2006.

Office of Management and Budget (OMB) memorandum M-05-04, "Policies for Federal Agency Public Websites," Dec. 17, 2004, <http://www.whitehouse.gov/omb/memoranda/fy2005/m05-04.pdf>.

TRADOC Command Guidance: Noble Eagle #02-019, *Personal Data on Unclassified Websites*, March 13, 2002.

Army Regulation 340-21, *The Army Privacy Program*, July 5, 1985, http://www.apd.army.mil/jw2/xmldemo/r340_21/cover.asp or http://www.apd.army.mil/pdffiles/r340_21.pdf.

Defense Privacy Office, <http://www.defenselink.mil/privacy/>.

Privacy policy example, <http://www.defenselink.mil/warning/warn-dl.html>.

PUBLIC KEY INFRASTRUCTURE (PKI)

Memorandum from the Assistant Secretary of Defense for Networks and Information Integration (ASD-NII), "Support for Information Assurance and Computer Network Defense (CND) Assessments, Priorities, Initiatives and Processes," April 7, 2004.

Department of Defense Instruction 8520.2, *Public Key Infrastructure (PKI) and Public Key Enabling*, April 1, 2004, <http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf>.

Memorandum from the Assistant Secretary of Defense, "Guidance and Provisions for Development Department of Defense (DoD) Components Public Key Enabling (PKE) Policy Compliance Waiver Process," Aug. 5, 2002.

Memorandum from DoD Chief Information Officer (CIO), Office of the Assistant Secretary of Defense, "Public Key Enabling (PKE) of Applications, Web servers and Networks for the Department of Defense (DoD)," May 17, 2001.

Memorandum from DoD Chief Information Officer, Office of the Assistant Secretary of Defense, "Department of Defense (DoD) Public Key Infrastructure (PKI)," Aug. 12, 2000.

RECORDS AND FILE MANAGEMENT

Army Regulation 25-400-2, *The Army Records Information Management System (ARIMS)*, Oct. 2, 2007, http://www.apd.army.mil/jw2/xmldemo/r25_400_2/cover.asp or http://www.apd.army.mil/pdf/r25_400_2.pdf.

TRADOC Regulation 25-1, *Information Resources Management*, Sept. 16, 2006 [currently being updated], <http://www.tradoc.army.mil/tpubs/regs/r25-1.pdf> or <http://www.tradoc.army.mil/tpubs/regs/r25-1.doc>. See Paragraph 5-4.

Office of Management and Budget (OMB) memorandum M-05-04, "Policies for Federal Agency Public Websites," Dec. 17, 2004, <http://www.whitehouse.gov/omb/memoranda/fy2005/m05-04.pdf>.

National Archives and Records Administration (NARA) documents, *Transfer Instructions for Permanent Electronic Records*, issued 2003-2004: Web content records, <http://www.archives.gov/records-mgmt/initiatives/web-content-records.html>; digital photographic records, <http://www.archives.gov/records-mgmt/initiatives/digital-photo-records.html>; PDFs, <http://www.archives.gov/records-mgmt/initiatives/pdf-records.html>.

Department of Defense Directive 5015.2, *DoD Records Management Program*, March 6, 2000, certified current as of Nov. 21, 2003, <http://www.dtic.mil/whs/directives/corres/pdf/501502p.pdf>.

Department of the Army Memorandum 25-51, "Records Management Program," July 24, 1995, http://www.apd.army.mil/pdf/m25_51.pdf.

Electronic Information Management standards Web portal, <http://www.archives.gov/records-mgmt/initiatives/standards.html>.

SECTION 508

Department of the Army Pamphlet 25-1-1, *Information Technology Support and Services*, Oct. 25, 2006, http://www.apd.army.mil/jw2/xmldemo/p25_1_1/cover.asp or http://www.apd.army.mil/pdf/p25_1_1.pdf. See Paragraphs 7-5, 8-3, and 8-7.

Office of Management and Budget (OMB) memorandum M-05-04, "Policies for Federal Agency Public Websites," Dec. 17, 2004, <http://www.whitehouse.gov/omb/memoranda/fy2005/m05-04.pdf>.

Electronic and Information Technology Accessibility Standards (Section 508), Dec. 21, 2000, <http://www.access-board.gov/sec508/standards.htm>.

Memorandum from the Office of the Assistant Secretary of Defense, "Accessibility of DoD Websites to People with Disabilities," July 21, 2000.

SECURITY / OPERATIONS SECURITY

Army Regulation 25-2, *Information Assurance*, rapid-action revision March 23, 2009, on regulation dated Oct. 24, 2007, http://www.apd.army.mil/pdf/r25_2.pdf.

Department of Defense Instruction 5230.29, *Security and Policy Review of DoD Information for Public Release*, Jan. 8, 2009, <http://www.dtic.mil/whs/directives/corres/pdf/523029p.pdf>.

All Army activities (ALARACT) message, "Website Security Policy Compliance," Dec. 19, 2008.

Department of Defense Manual 5205.02-M, *DoD Operations Security (OPSEC) Program Manual*, Nov. 3, 2008, <http://www.dtic.mil/whs/directives/corres/pdf/520502m.pdf>.

Department of Defense Instruction 5200.01, *DoD Information Security Program and Protection of Sensitive Compartmented Information*, Oct. 9, 2008, <http://www.dtic.mil/whs/directives/corres/pdf/520001p.pdf>.

Memorandum from the Deputy Secretary of Defense, "Department of Defense (DoD) Website Security Policy Compliance," Sept. 25, 2008, and the Secretary of the Army's undated executive-summary response.

Army Regulation 525-13, *Antiterrorism*, Sept. 11, 2008, https://akocomm.us.army.mil/usapa/epubs/DR_pubs/DR_b/xml/r525_13/cover.xml or https://akocomm.us.army.mil/usapa/epubs/dr_pubs/dr_b/pdf/r525_13.pdf (FOUO; AKO log-in required).

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3213.01C, *Joint Operations Security*, July 17, 2008, http://www.dtic.mil/cjcs_directives/cdata/unlimit/3213_01.pdf.

All Army activities (ALARACT) message 089/2008, "Securing AKO Content and Credentials (NIPR)," March 25, 2008.

Department of Defense Directive 8500.01E, *Information Assurance (IA)*, Oct. 24, 2002, certified current as of April 23, 2007, <http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf>.

Army Regulation 530-1, *Operations Security*, April 19, 2007 [currently being updated], https://akocomm.us.army.mil/usapa/epubs/dr_pubs/DR_c/pdf/r530_1.pdf or https://akocomm.us.army.mil/usapa/epubs/dr_pubs/DR_c/xml/r530_1/cover.xml (FOUO; AKO log-in required).

Department of Defense Instruction 8552.01, *Use of Mobile Code Technologies in DoD Information Systems*, Oct. 23, 2006, <http://www.dtic.mil/whs/directives/corres/pdf/855201p.pdf>.

All DoD activities (ALDODACT) message 11/06 (joint message from Deputy Secretary of Defense / Vice Chairman of the Joint Chiefs of Staff), "Information Security / Website Alert," Aug. 9, 2006, <http://www.defenselink.mil/webmasters/policy/infosec20060806.html>.

TRADOC Operations Security (OPSEC) Plan, July 10, 2006.

Department of Defense Directive 5205.02, *DoD Operations Security (OPSEC) Program*, March 6, 2006, <http://www.dtic.mil/whs/directives/corres/pdf/520502p.pdf>.

Joint Publication 3-13, *Information Operations*, Feb. 13, 2006, http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf.

All Army activities (ALARACT) message 156/2005 from Chief of Staff of the Army (CSA), "Chief of Staff of the Army OPSEC Guidance," Aug. 23, 2005.

TRADOC supplement to Army Regulation 25-2, *Information Assurance*, Aug. 18, 2005, <http://www.tradoc.army.mil/tpubs/pdf/suppl/s25-2.pdf>.

All Army activities (ALARACT) message (included in 156/2005) from Vice Chief of Staff of the Army (VCSA), "Sensitive Photos," Feb. 14, 2005.

Department of Directive 8570.01, *Information Assurance (IA) Training, Certification, and Management*, Aug. 15, 2004, <http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf>.

OPSEC Notice to All Army Personnel (ONTAP) 04-01, "Security Classification Guidance (SCG) Extended for Operation Iraqi Freedom to Include Tactical Maneuver Plans and Operational Execution to Classification SECRET," March 9, 2004.

Field Manual 3-13, *Information Operations: Doctrine, Tactics, Techniques and Procedures*, Nov. 28, 2003, https://akocomm.us.army.mil/usapa/doctrine/DR_pubs/dr_aa/pdf/fm3_13.pdf.

All Army activities (ALARACT) message, "Army-wide Website OPSEC Review," Feb. 28, 2003.

Department of Defense Instruction 8500.2, *Information Assurance (IA) Implementation*, Feb. 6, 2003, <http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf>.

Message from the Secretary of Defense, "Website OPSEC Discrepancies" (ALDODACT 02/03), Jan. 14, 2003, http://www.defenselink.mil/webmasters/policy/rumsfeld_memo_to_DOD_webmasters.html.

Memorandum from the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD-C3I), "Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites," Dec. 28, 2001, http://www.defenselink.mil/pubs/foi/names_removal.pdf.

Memorandum from the Deputy Secretary of Defense, "Operations Security throughout the Department of Defense," Oct. 18, 2001, included at http://www.defenselink.mil/pubs/foi/names_removal.pdf (last memo).

Army Regulation 380-5, *Department of the Army Information Security Program*, Sept. 29, 2000, http://www.apd.army.mil/jw2/xmldemo/r380_5/cover.asp or http://www.apd.army.mil/pdf/r380_5.pdf.

Memorandum from the Deputy Secretary of Defense, “Information Vulnerability and the Worldwide Web,” Sept. 24, 1998, http://www.defenselink.mil/other_info/depsecweb.pdf.

Joint Publication 3-07.2, *Joint Tactics, Techniques and Procedures for Antiterrorism*, March 17, 1998, http://www.dtic.mil/doctrine/jel/new_pubs/jp3_07_2.pdf.

Joint Publication 3-54, *Joint Doctrine for Operations Security*, Jan. 24, 1997, http://www.dtic.mil/doctrine/jel/new_pubs/jp3_54.pdf.

National Security Decision Directive No. 298, *National Operations Security Program*, Jan. 22, 1988, <http://www.iooss.gov/nsdd298.pdf>.

Information Assurance Support Environment (IASE) (DoD IA portal), <http://iase.disa.mil/ind>

Appendix B Glossary

Section I

Acronyms

AAR – after-action report
AASA – Administrative Assistant to the Secretary of the Army
ACOM – Army command
AFB – air force base
AKM – Army Knowledge Management
AKO – Army Knowledge On-line
ALARACT – all Army activities
ALDODACT – all Department of Defense activities
AMC – U.S. Army Material Command
AP – Associated Press
APD – Army Publishing Directorate
APS – Army Prepositioned Stocks
AR – Army regulation
ARCIC – Army Capabilities Integration Center
ARI – Army Research Institute
ARNG – Army National Guard
ASD-C3I – Assistant Secretary of Defense for Command, Control, Communications and Intelligence
ASD-NII – Assistant Secretary of Defense for Networks and Information Integration
ASD-PA – Assistant Secretary of Defense for Public Affairs
AWRAC – Army Web Risk Assessment Cell
BCKS – Battle Command Knowledge System
BCT – basic combat training
Blog – Web log
BRAC – base realignment and closure
C2 – command and control
C4 – command, control, communications, and computers
C4I – command, control, communications, computers, and intelligence
CAC – Common Access Card
CD – compact disc
CE – civilian enterprise
CFR – Code of Federal Regulations
CG – commanding general
CI – command information
CI – counterintelligence
CIO – Chief Information Office(r)
CJCS – Chairman of the Joint Chiefs of Staff
CJCSI – Chairman of the Joint Chiefs of Staff Instruction
COA – course of action
CoE – center of excellence
COMPUSEC – computer security
COMSEC – communications security
CONOPS – concept of operations
CONUS – continental United States
COOP – continuity-of-operations plan
CPA – Chief of Public Affairs
CSA – Chief of Staff, Army
CUI – controlled unclassified information
DA – Department of the Army
DAA – designated approving authority
DA&M – DoD Administration and Management

DA PAM – Department of the Army pamphlet
DASD – Deputy Assistant Secretary of Defense
DCG – deputy commanding general
DCS – deputy chief of staff
DDIE – Department of Defense Information Enterprise
DEPSECDEF – Deputy Secretary of Defense
DISC4 – Director(ate) of Information Systems for Command, Control, Communications and Computers (former name of Army CIO)
DKO – Defense Knowledge On-line
DMZ – demilitarized zone
DoD – Department of Defense
DoDD – Department of Defense Directive
DOIM – Director(ate) of Information Management
DoDI – Department of Defense Instruction
DoJ – Department of Justice
DOO – DoD originating office
DoS – Department of State
Dpi – dots per inch
DRU – direct reporting unit
EEFI – Essential Elements of Friendly Information
EIT – electronic and information technology
EO – executive order
FAQ – frequently asked questions
FD – foreign disclosure
FIPS – Federal Information-Processing Standard
FISMA – Federal Information Security Management Act
FOA – field operating activity
FOIA – Freedom of Information Act
FORSCOM – U.S. Army Forces Command
FOUO – For Official Use Only
FTP – File Transfer Protocol
GIG – Global Information Grid
GO – general officer
HQ – headquarters
HTML – Hypertext Markup Language
HTTP – Hypertext Transfer Protocol
HTTPS – Hypertext Transfer Protocol-Secure
Hz – hertz
IA – information assurance
IAW – in accordance with
IED – improvised explosive device
IG – Inspector General
IIA – interactive Internet activities
IMCOM – Installation Management Command
IMT – initial military training
INFOSEC – information security
INSCOM – Intelligence and Security Command
IO – information operations
IOC – 1st Information Operations Command
IOSS – Interagency OPSEC Support Staff
IP – Internet protocol
IRM – information-resources management
IS – information system
ISP – Internet service provider
ISR – intelligence, surveillance, and reconnaissance
IT – information technology

ITAR – International Traffic in Arms Regulation
JER – Joint Ethics Regulation
JP – Joint publication
JTA – Joint Technical Architecture
JTF-GNO – Joint Task Force-Global Network Operations
KC – knowledge center
KIA – killed in action
LDAP – Lightweight Directory Access Protocol
LE – law enforcement
LEA – Law Enforcement Agency
LOC – lines of communication
MANSCEN – Maneuver Support Center
MEOC – minimum essential operational capability
MILDEP – military department
MOS – military-occupation specialty
MSO – major subordinate organization
MTOE – modified table of organization and equipment
MTT – mobile training team
MWR – morale, welfare and recreation
NARA – National Archives and Records Administration
NBC – nuclear, biological, and chemical
NCA – national command authority
NCO – noncommissioned officer
NDU – National Defense University
NIH – National Institutes of Health
NIPRNET – Non-Secure Internet Protocol Routed Network
NIST – National Institute of Standards and Technology
NSA – National Security Agency
NSS – national-security system
OASD-PA – Office of the Assistant Secretary of Defense for Public Affairs
OCPA – Office Chief of Public Affairs
OMB – Office of Management and Budget
OMEMS – Ordnance Mission and Electronic Maintenance School
OMMS – Ordnance Mechanical Maintenance School
ONTAP – OPSEC Notice to All Army Personnel
OPCON – operational control
OPLAN – operational / operations plan
OPORD – operational order
OPSEC – operations security
OSD – Office of the Secretary of Defense
OSMD – On-line and Social Media Division (part of OCPA)
OSR – Office of Security Review
OWG – OPSEC Working Group
P3P – Platform for Privacy Preferences Project
PA – privacy advisory
PAO – Public Affairs Office(r)
PAS – Privacy Act statement
PDA – portable digital assistant
PDF – Portable Document Format
PED – portable electronic device
PII – personally identifying information
PKI – Public Key Infrastructure
PM – personnel misconduct
POC – point of contact
PRA – Paperwork Reduction Act
PSYOP – psychological operations

QDR – Quadrennial Defense Review
QI – quality of information
RDT&E – research, development, test, and evaluation
RMDA – Records Management and Declassification Agency
ROTC – Reserve Officers Training Corps
SAP – Special Access Program
SBU – sensitive but unclassified
SCG – security classification guidance
SCIG – Strategic Communication Integration Group
SecArmy – Secretary of the Army
SECDEF – Secretary of Defense
SES – Senior Executive Service
SIPRNET – secure Internet protocol routed network
SIR – serious-incident report
SJA – Staff Judge Advocate
SME – subject-matter expert
SMTP – Simple Mail Transfer Protocol
SNS – social-networking site
SOF – Special Operations Forces
SOP – standard operating procedure; standing operating procedure
SSL – Secure Sockets Layer
SSN – Social Security number
SSO – single sign-on
SWOT – strengths, weaknesses, opportunities, and threats
TAQ – Total Army Quality
TCP – Transmission Control Protocol
TDA – table of distribution and allowances
TKE – TRADOC Knowledge Environment
TLD – top-level domain
TRADOC – U.S. Army Training and Doctrine Command
TR – TRADOC regulation
TTP – tactics, techniques, and procedures
UCMJ – Uniform Code of Military Justice
URL – Uniform Resource Locator
USAAC – U.S. Army Accessions Command
USACAC – U.S. Combined Arms Center
USACASCOM – U.S. Army Combined Arms Support Command
USACC – U.S. Army Cadet Command
USAR – U.S. Army Reserve
USAREC – U.S. Army Recruiting Command
USASOC – U.S. Army Special Operations Command
USC – U.S. Code
US-CERT – U.S. Computer Emergency Response Team
USG – U.S. government
USMA – United States Military Academy
VAD – Vulnerabilities Assessment Division
VCJCS – Vice Chairman of the Joint Chiefs of Staff
VCSA – Vice Chief of Staff of the Army
VI – visual information
VIDOC – visual-information documentation
VIP – very important person
W3C – Worldwide Web Consortium
WAI – Web Accessibility Initiative
WCAG – Web Content Accessibility Guidelines
WCWG – Web Content Working Group
WHS – Washington Headquarters Services

WIS – Web information service
WWG – Webmaster Working Group
WWPAS – Worldwide Public Affairs Symposium
WWW – Worldwide Web

Section II Definitions



Access control

A means for managers of ISs to exercise a directing or restraining influence over the behavior, use, and content of a system, and to specify what authorized users can do, which resources they can access, and what operations they can perform. Access controls limit access to content on a Webserver, using means such as user authentication and firewalls. Adequate security and access controls must be employed for information determined to place national security, DoD personnel and assets, mission effectiveness, or the privacy of individuals at an unacceptable level of risk. Determinations as to the appropriate security and access controls to employ will be based upon the sensitivity of the information, the target audience for which the information is intended, and the level of risks to DoD interests. [Section II of glossary, AR 25-1; Section II of glossary, AR 25-2]

The positive access controls of CAC / PKI will be used to control access to content that is FOUO and SBU. Data classified as *confidential* or *secret* must be transmitted over a network with a minimum security classification of *secret*, such as on the SIPRNET. [Paragraph 5-3b(2), TR 25-1]

Domain and / or IP address restriction is not an effective method of access control. Such restrictions are easily defeated. The current version of the Security Technical Information Guide (STIG), “Access Control in Support of Information Systems,” published by the Defense Information Systems Agency (DISA) at <http://iase.disa.mil/stigs/stig>, provides guidance. [DoDI 8410.1]

Adversary

Anyone who wants access to your information or your system and is willing to act against you to get it.

Individuals, organizations, or countries that must be denied critical information to preserve mission integrity and maintain friendly mission effectiveness and the element of surprise. Adversary, in this context, includes any individual, organization, or country with which specific information should not be shared to preserve mission integrity or the element of surprise. [Glossary, DoD Manual 5205.02-M; Section II of glossary, AR 530-1]

Army information

Information originated by or concerning the Army. [Section II of glossary, AR 25-2]

Army Public Affairs

Dissemination of accurate information about Army matters of general interest or concern to the public not inconsistent with security, and interactive communication with Army publics to enhance mutual understanding and respect. [Section II of glossary, AR 360-1]

Army Web Risk Assessment Cell

A team of IA personnel who conduct ongoing OPSEC and threat assessments of Army publicly accessible Websites to ensure compliance with DoD and Army policy and best practices. [Section II of glossary, AR 25-1]

Army Website

A collection of HTML pages, graphics, images, video, audio, databases, or other media assets at a URL which is made available for distribution and / or distributed or transmitted (with or without limitation) via the WWW for reception and display on a computer or other devices including, but not limited to, mobile phones, PDAs, or interactive TV. Content is controlled, authorized, or sponsored by an Army organization or representative. [Section II of glossary, AR 25-1]

Authenticate

To verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to possible unauthorized modification in an IS. To establish the validity of a transmitted message. [Section II of glossary, AR 25-2]

Authentication

A security measure designed to establish the validity of a transmission, message, or originator. A means of verifying an individual's identity or eligibility to receive specific categories of information or to perform specific actions. [Section II of glossary, AR 25-1; Section II of glossary, AR 25-2]

Authenticator

Something the user knows, such as a unique password; something the user possesses, such as a token (CAC); or a physical characteristic (biometric).



Benchmark

A procedure, problem, or test that can be used to compare systems, components, processes, and so forth to each other or to a standard. [Section II of glossary, AR 25-1]

A point of reference from which measurements may be made. The term refers to the process of finding and adapting best practices and performance for similar activities, inside or outside an organization, to improve organizational performance. This represents a strategic and analytic process of continuously measuring an organization's products, services, and practices against a recognized leader in the studied area. [Section II of glossary, AR 5-1]

Best practice

A superior method or innovative process that contributes to improved performance. [Section II of glossary, AR 5-1]

Blog

See *Web log*.

Business practice

A specific, well defined, set of activities performed by an organization that create value for the customer and results in accomplishing a stated goal. [Section II of glossary, AR 25-1]



Center of excellence

Designated training center based on TRADOC core functions (IMT, functional training, leader development and education, lessons learned, collective training, doctrine, training support, concepts, experimentation, and requirements determination) that improves combined-arms solutions for Joint operations; fosters doctrine, organizations, training, materiel, leader development, personnel and facilities (DOTMLPF) integration; accelerates the development process; and unites all aspects of institutional training to develop Soldiers, leaders, and civilians who embody Army values.

Designated by HQ DA, a center of excellence is a premier organization that creates the highest standards of achievement in an assigned sphere of expertise by generating synergy through effective and efficient combination and integration of functions while reinforcing unique requirements and capabilities. [Section II of glossary, AR 5-22]

Civilian-enterprise publications

Newspapers, magazines, installation guides, installation maps, and Websites that support command internal communications. The PAO provides oversight and final approval authority for the publication's editorial (news, information, photographs, editorials, and other materials) content. CE publications contain advertising sold by the civilian printer and may include supplements or inserts. CE publications authorized by AR 360-1 are the only Army

PA publications allowed to contain paid advertisements on a regular basis. MWR may sell advertising under some circumstances outlined in DoDI 1015.10, Enclosure 10. [Paragraphs 3-5c, 3-5o, 3-5u, 13-5a, 13-5b, and 13-5d, AR 360-1]

Classified defense information

Official information regarding the national security that has been designated *top secret*, *secret*, or *confidential* IAW EO 12958, as amended, and EOs 12972, 13142, and 13292. [Section II of glossary, AR 25-2]

See also the definition for *classified military information*, IAW Section II of glossary, AR 530-1: Information originated by or for DoD or its agencies, or under their jurisdiction or control, that requires protection in the interest of national security. It is designated *top secret*, *secret*, or *confidential* as described in EO 12958 or subsequent order. Classified military information may be in oral, visual, documentary, or materiel form.

Clearance of information

Approval by the reviewing authority to publish or release submitted material. (PAO is the final reviewing authority in clearing Web content.) [Section II of glossary, AR 360-1]

Command / activity public affairs office(r)

A Public Affairs position, preferably on a TRADOC Table of Distribution and Allowances (TDA), that provides essential, focused, organic support to a TRADOC mission activity – i.e., a TRADOC MSO, CoE, center / school, FOA, or other organization subordinate to HQ TRADOC. Typically the command / activity PAO is integrated with and supported by the garrison PAO. When a senior leader at an installation is dual-hatted as the senior commander and the TRADOC mission commander, the command / activity PAO and the senior commander's PAO are usually the same individual.

Command information

The ability to communicate with members of the military departments, civilian employees, contractors, and family members of the Joint forces deployed and at home bases, to create awareness of the goals and significant developments affecting deployed forces. [Glossary, DoDI 5400.13]

Combat camera

VI documentation covering air, sea, and ground actions of members of the military departments who are in combat or combat support operations, humanitarian operations and related peacetime training activities, such as exercises, wargames and operations, in support of the office of the CJCS and the combatant commands. [Glossary, DoDI 5400.13]

Contingency plan

A plan maintained for emergency response, backup operations, and post-disaster recovery for an IS, as a part of its security program, that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. [Section II of glossary, AR 25-2]

Cookie

A small piece of information (mechanism or token) about a user sent by a Webserver and stored on the user's own computer so it can later be read back from that computer. Cookies are embedded in the HTML information flowing back and forth between the user's computer and the servers. They allow user-side customization of Web information. Cookies may be categorized as *session* or *persistent* cookies. Session cookies are temporary cookies that are used to maintain context or "state" between otherwise stateless Web transactions (for example, to maintain a "shopping basket" of goods selected during a single logical session at a site), and they normally expire (and are deleted) at the end of the Web session in which they are created. Persistent cookies remain over time and can be used for a variety of purposes, including tracking a user's access over time and across Websites, establishing user preferences, and collecting personal information. [Part III, DoD Web policy; Section II of glossary, AR 25-1]

Controlled unclassified information

Types of information that require application of controls and protective measures, for a variety of reasons, not to include those that qualify for formal classification. (See definition of "classified defense information," above.) Unclassified information to which access or distribution limitations have been applied according to national laws,

policies, and regulations of the U.S. government; this includes U.S. information that is determined to be exempt from public disclosure according to DoDD 5230.25, DoDD 5400.7, AR 25-55, AR 340-21, AR 530-1, and so on, or that is subject to export controls according to the International Traffic in Arms Regulation (ITAR) or the Export Administration Regulations (EAR). Because CUI does not qualify for formal classification, it should be afforded OPSEC measures for additional protection because of its vulnerability as unclassified information. For examples of CUI, see Appendix F. [Section II of glossary, AR 380-5; Paragraph 1-5c(3)(b), AR 530-1; Paragraph 1-4e(10) and Section II of glossary, AR 380-10]

Core competencies

The knowledge and skills needed within the workforce to perform an important business function of the organization. Core competencies directly relate to mission and customer service and are those processes and functions that could not be out-sourced without substantially weakening the organization. [Section II of glossary, AR 25-1]

Critical information

Information important to the successful achievement of U.S. objectives and missions, or which may be of use to an adversary of the United States. Critical information consists of specific facts about friendly activities, intentions, capabilities, or limitations an adversary needs to gain a military, political, diplomatic, or technological advantage, or for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. It is information that is vital to a mission that – if an adversary obtains it, correctly analyzes it, and acts upon it – the compromise of this information could prevent or seriously degrade mission success. The identification of critical information is important in that it focuses the remainder of the OPSEC process on protecting vital information rather than attempting to protect all classified or sensitive information.

Critical information can be classified information or unclassified information. Critical information that is classified requires OPSEC measures for additional protection because it can be revealed by unclassified indicators. Critical information that is unclassified especially requires OPSEC measures because it is not protected by the requirements provided to classified information.

Critical information may be identified by answering these questions: 1) Who is the adversary? (Who has the intent and capability to take action against the United States and its allies? 2) What are the adversary's goals? (What does the adversary want to accomplish?) 3) What is the adversary's strategy? (What actions might the adversary take?) 4) What critical information does the adversary already know? (What information is it too late to protect?) 5) What are the adversary's intelligence-collection capabilities (available from the organization's counterintelligence and intelligence organization)?

Critical information can also be an action that provides an indicator of value to an adversary and places a friendly activity or operation at risk. Indicators that would reveal critical information are also critical information.

The term "critical information" has superseded the term "Essential Elements of Friendly Information" (EEFI) as used in FM 3-13. EEFI now refers to critical information phrased in the form of a question to protect classified and sensitive information.

Examples of critical information are at Appendix E. [CJCSI 3213.01C; Paragraphs 1c and 2a of Chapter III, Appendix A, Paragraph 2 of Appendix C, and Part II of glossary, Joint Publication (JP) 3-54; JP 1-02; Paragraphs 1-5b, B-2, Appendix C and Section II of glossary, AR 530-1; Chapter 3, FM 3-13]

Countermeasure

Anything that effectively negates or mitigates an adversary's ability to exploit vulnerabilities. [Glossary, DoD-M 5205.02]

Customer

Anyone for whom an organization or individual provides goods or services, or a person or group who uses the output of a process. External customers reside outside the producing organization. Internal customers reside inside the producing organization. [Section II of glossary, AR 5-1]



Data asset

Any entity that comprises data, such as a system file, database, document, official electronic record, image, audio file, Website, and data-access service. A data asset also includes a service that may be provided to access data from an application, such as a Website that returns data in response to specific queries (for example, www.weather.com). Data assets are the core of the Army's net-centric environment, to enable effective and timely decisions. [Paragraph 5-2b(1) and Section II of glossary, DA PAM 25-1-1. See also Paragraph 5-2d, DA PAM 25-1-1]

Data mining

The nontrivial extraction of implicit, previously unknown, and potentially useful information from data. Data mining uses machine learning, statistical, and visualization techniques to discover and present knowledge in a form that is easily comprehensible to humans. [Paragraph 3.5.2.1, Part II, DoD Web policy]

Demilitarized zone

A small network or computer host that serves as a "neutral zone" between an internal network and the public network. A DMZ prevents users from obtaining direct access to an internal server that may have business data on it. A DMZ is another approach to the use of a firewall and can act as a proxy server if desired. [Section II of glossary, AR 25-2]

IAW Paragraphs 4-20g(12) and (13), AR 25-2, Army organizations are to protect publicly accessible Websites by placing them behind an Army reverse Web proxy server, or if not available, on a DMZ as a form of protection. The proxy server and DMZ, however, are not positive access controls in that they do not require authentication from the client/user in the form of the CAC login, biometric, or other unique, individual authenticator.

Department of Defense Information Enterprise

The DoD information resources, assets, and processes required to achieve an information advantage and share information across DoD and with mission partners. The DDIE includes: (a) the information itself and DoD's management over the information lifecycle; (b) the processes, including risk management, associated with managing information to accomplish the DoD mission and functions; (c) activities related to designing, building, populating, acquiring, managing, operating, protecting, and defending the information enterprise; and (d) related information resources such as personnel, funds, equipment, and IT, including national-security systems. [Glossary, DoDD 8000.01]

Direct reporting unit

An operational command that reports to and is under the direct supervision of an HQ DA element. A DRU executes its unique mission based on policy established by its HQ DA principal. [Section II of glossary, AR 25-1]

Disclosure

The furnishing of information about an individual, by any means, to an organization, government agency, or to an individual who is not the subject of the record, the subject's designated agent or legal guardian. Within the context of the Privacy Act and AR 340-21, this term applies only to personal information that is a part of a *system of records*. [Section II of glossary, AR 340-21]

DoD personnel

For purposes of defining who must submit information into the review process for clearance, DoDD 5230.9 applies to all DoD personnel (IAW Paragraph 2a(2)). The term *DoD personnel* includes any DoD civilian officer or employee (including special government employees) of any DoD component (including any non-appropriated-fund activity); any active-duty Regular or Reserve military officer, warrant officer, and active-duty enlisted member of the Army, Navy, Air Force or Marine Corps; any Reserve or National Guard member on active duty under orders issued IAW Title 10, U.S. Code; any Reserve or National Guard member performing official duties, including while on inactive duty for training or while earning retirement points, or while engaged in any activity related to the performance of a federal duty or function; any faculty member in a civil-service position or hired under Title 10, and any student (including a cadet or midshipman) of an academy, college, university or school of DoD; and any foreign

national working for a DoD component except those hired for a defense contract, consistent with labor agreements, international treaties and agreements, and host-country laws. [Glossary, DoDD 5230.9]

Dissemination of information

Component-initiated or -sponsored distribution of information to the public. *Dissemination* does not include:

- Distribution of information that is limited to government employees, DoD contractors, or grantees;
- Intra- or inter-DoD use or sharing of government information, including responses to requests under the FOIA, the Privacy Act, the Federal Advisory Committee Act, or other similar laws;
- Distribution of correspondence with individuals or persons;
- Information limited to subpoenas and adjudicative processes;
- Information that has previously been disseminated to the public and is subsequently presented to Congress as part of the legislative or oversight processes, including testimony of officials, and information or drafting assistance provided to Congress in connection with pending or proposed legislation;
- Press releases and other information advising the public of an event or activity;
- Procedural, operational, policy, and internal manuals prepared for the management and operations of the component that are not primarily intended for public dissemination, including personnel notices such as vacancy announcements;
- Information that is not otherwise disseminated to the public.

With the exception of press releases, none of the limited information is appropriate for the general public and therefore will not be posted to publicly accessible Websites. If disseminated, the standards of information quality apply, except for press releases – QI exemption is given to press releases and other information advising the public of an event or activity – but not to stories that do not advise the public of an event or activity. Further, the QI exemption for press releases and similar information applies only to information that is disseminated under urgent situations, including imminent or credible threats to national defense and security. [Paragraphs 2 and 4.1, Attachment 2, memorandum from the DEPSECDEF, “Ensuring Quality of Information Disseminated to the Public by the Department of Defense”]

Domain / domain name

A set of network addresses, organized in levels. The top level identifies geographic or purpose commonality (for example, the nation the domain covers or a category such as “commercial” (.com) or “military” (.mil)). The second level identifies a unique place within the top-level domain (TLD) and is, in fact, equivalent to a unique address on the Internet (or IP). Lower levels of domain may also be used. For purposes of data-sharing in DoD, domains are subsets of mission areas and represent a common collection of related, or highly dependent, information capabilities and services. [Section II of glossary, DA PAM 25-1-1]

In the Domain Name System (DNS) naming of computers, there is a hierarchy of names and a set of TLDs. These are the generic TLDs and the two-letter country codes from International Organization for Standardization (ISO) Standard Number 3166. A hierarchy of names usually exists under each TLD. For example, .mil is a TLD, .osd.mil is a second-level domain (SLD), and [tricare.osd.mil](#) is a third-level domain (not usually referred to with an acronym). The TLDs of .mil and .gov are restricted to use by entities in the United States; .mil is for the Defense Department’s exclusive use. [Enclosure 2, DoDI 8410.1]

For determination of records, [www.tradoc.army.mil](#) and [www.tradoc.army.mil/pao/](#) are both in the same site or domain, but [www.usda.gov](#) and [www.nal.usda.gov](#) require separate records, since one is registered as a primary domain and the other as a secondary domain. [Glossary at <http://www.archives.gov/records-mgmt/initiatives/web-content-records.html>, accessed June 9, 2006] For purposes of Web-content records, domain defines the administrative boundaries and content of an agency’s Website unless a formal Web-management agreement specifically allows agency content to reside on a non-agency domain. In which case, content hosted at the non-agency domain is also included as part of the agency’s Web content. [<http://www.archives.gov/records-mgmt/initiatives/web-content-records.html>, accessed June 9, 2006]



Electronic government

The use by government of Web-based Internet applications and other information technologies, combined with processes that implement these technologies, to (a) enhance the access to and delivery of government information and services to the public, other agencies, and other government entities; or (b) bring about improvements in government operations that may include effectiveness, efficiency, service quality, or transformation. [Section II of glossary, AR 25-1]

Electronic signature

A generic term encompassing both non-cryptographic and cryptographic methods of authenticating identity. Non-cryptographic methods include personal identification number (PIN) or password, smart card, digitized signature, and biometrics. Cryptographic methods include shared symmetric key cryptography, and public/private key (asymmetric) cryptography-digital signatures. [Section II of glossary, AR 25-1]

Essential Elements of Friendly Information

Key questions likely to be asked by adversary officials and intelligence systems about friendly capabilities, activities, limitations, and intentions so they can obtain answers critical to their operational effectiveness. [Paragraph 1c, Chapter III, and Part II of glossary, JP 3-54; Section II of glossary, AR 530-1]

The EEFI is critical information phrased in the form of a question that does not reveal the details of critical information to prevent disclosure of classified and sensitive information. EEFI are phrased as questions that the adversary is likely to ask about friendly capabilities, activities, limitations, and intentions. The use of EEFI is an effective way to ensure the widest dissemination of a unit or organization's critical information while protecting classified and sensitive information. *Critical information* supersedes the term *essential elements of friendly information* as used in FM 3-13 (see the following paragraph). DoD and the service components are now using the term *critical information* for the purpose of standardization. The Army will continue to use the term EEFI in modified purpose related to critical information. [Section II of glossary, AR 530-1]

The Army defines EEFI as the critical aspects of a friendly operation that, if known by the enemy, would subsequently compromise, lead to failure, or limit success of the operation, and therefore must be protected from detection. Army doctrine defines EEFI differently from Joint doctrine. The Joint definition focuses on information that adversaries want to collect. The Army definition focuses on information that friendly commanders want to protect. The Joint definition of EEFI includes friendly information that may not compromise friendly operations. Army OPSEC doctrine addresses protecting information that is relevant from the adversary's perspective; it does not address what Joint doctrine considers EEFI. [Chapter 3, FM 3-13]

Essential secrecy

The condition achieved by the denial of critical information to adversaries. Essential secrecy depends on the combination of two approaches to protection: security programs to deny adversaries classified information, and OPSEC programs to deny adversaries critical information and indicators of sensitive information. [Paragraph 1-6b and Section II of glossary, AR 530-1]

External link

A hyperlink from an Army Website to a source external to one's organization and outside an official DoD Website (usually external to the .mil domain). A disclaimer is required when an external link is made. [Paragraphs 7.1 and 7.2, Part II, DoD Web policy]

Extranet

A private network that uses Internet protocols and the public telecommunications system to securely share information among selected external users. An extranet requires the use of firewalls, authentication, encryption, and VPNs that tunnel through the public network. [Section II of glossary, AR 25-2]



Facebook

An on-line community (Website) for people to connect or re-connect with others. Enables people to share videos, pictures, and information about themselves. One of the fastest growing social networks of the past two years. www.Facebook.com.

Family member

A family member – or *dependent* as defined by USC 1072(2) – is the spouse; unremarried widow or widower; or unmarried legitimate child – including adopted child, stepchild, foster child, or ward – of a current or former DoD civilian employee or military service member. *Child* is further defined as someone 1) under age 21, 2) incapable of self-support because of a mental or physical incapacity that existed before his/her 21st birthday, or 3) under age 23 and enrolled in a full-time educational institution. [Section II of glossary, AR 215-1; Section II of glossary, AR 525-13]

A child under the age of 19 or any other member who depends upon the sponsor for total support and or care. [Section II of glossary, AR 600-20]

Includes those individuals for whom the Soldier provides medical, financial, and logistical (for example, housing, food, and clothing) support. This includes, but is not limited to, the spouse, children under age 18, elderly adults, and persons with disabilities. [Section II of glossary, TR 1-8]

A dependent can also be a parent or parent-in-law dependent on a military sponsor for one-half of his / her support and residing in the sponsor's household. See AR 215-1 for more specifics. For the purposes of reviewing for prohibited PII, biographies of official command spokespersons will not mention marital status or refer to any family member, whether spouse, child, parent, or any other relation. News coverage of family members in on-line installation newspapers will be considered for OPSEC risk.

File Transfer Protocol

A Transmission Control Protocol (TCP) / IP service that supports bidirectional transfer of binary and ASCII files without loss of data between local and remote computers on the Internet. The FTP command set allows a user to log onto a remote server over the network, list file directories and copy files. [Section II of glossary, DA PAM 25-1-1]

For purposes of Web-content records, Web content is limited to what is accessed over HTTP. All other transfer protocols (i.e., FTP and Simple Mail Transfer Protocol (SMTP)) are excluded. [<http://www.archives.gov/records-mgmt/initiatives/web-content-records.html>, accessed June 9, 2006]

Firewall

A system or group of systems that enforces an access control policy between two networks with the properties of allowing only authorized traffic to pass between the networks from inside and outside the controlled environment and is immune to penetration. [Section II of glossary, AR 25-2]

Flickr

On-line scrapbook for storing, sharing, and commenting on photos. The Website provides limited photo-editing capabilities. It also allows contributors to place photos in individual albums or “sets” that can be categorized. <http://www.flickr.com>.

For Official Use Only

DoD information that is not classified *confidential* or higher IAW DoD 5200.1-R. For purposes of Web content, FOUO is a designation that is applied to unclassified information which is exempt from mandatory release to the public under eight of the nine exemptions to the FOIA (implemented by DoD 5400.7-R and AR 25-55). (The ninth FOIA exemption is for classified information; by definition, information must be unclassified to be FOUO.) FOUO information, though unclassified, nonetheless is sensitive and warrants protection from disclosure. FOUO is not a classification, as FOUO information is unclassified, but FOUO is not to be released to the public without undergoing a FOIA and/or legal review. FOUO will be the standard marking for all unclassified products that meet one or more of the exemptions of FOIA, and which if released to the public, could cause harm to Army operations or personnel.

Examples of FOUO information are at Appendix G. [Paragraphs 5-2a and 5-2b, AR 380-5; Paragraph 1-5c and Section II of glossary, AR 530-1]



Global Information Grid

The globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policymakers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national-security systems. Non-GIG IT includes stand-alone, self-contained, or embedded IT that is not, and will not be, connected to the enterprise network. [Glossary, DoDD 8000.01]

Graphic art

Hand-, mechanically, or computer-designed / created and -prepared two- or three-dimensional artworks or pictorial representations that are created rather than recorded in a camera. Includes charts, photo illustrations, photo montages, computer-generated pictures, drawings, paintings, animation cels, statues, bas-reliefs, graphs, icons, or logos for visual products such as brochures, posters, covers, television, motion pictures, printed publications, displays, presentations, and exhibits prepared manually, by machine, or by computer. Any item of graphic art prepared for release on the publicly accessible Web is Web content and as such will be submitted for the Web-content-review process. [Enclosure 1, memorandum from the ASD-PA, “Visual Information (VI) Activity Management”; Section II of glossary, AR 25-1]



Hazard

A condition with the potential to cause injury, illness or death of personnel; damage to, or loss of, equipment or property; or mission degradation. [Paragraph 3-23, Chapter 3, FM 3-13]

Homepage or “home page”

The single, top-level Webpage designed to be the first file accessed by a user visiting a Website; also known as an *index* or *default* page. [Part III, DoD Web policy; Section II of glossary, AR 380-5. Also, memorandum from Directorate of Information Systems for Command, Control, Communications and Computers (DISC4), “Guidance for Management of Publicly Accessible U.S. Army Websites”]

Hypertext Markup Language

Authoring software language used on the Internet and for creating Webpages. HTML is essentially text with embedded HTML commands identified by angle brackets and known as HTML tags. [Section II of glossary, DA PAM 25-1-1]

Hypertext Transfer Protocol

The communications protocol used by a Web browser to connect to Web servers on the Internet. [Section II of glossary, DA PAM 25-1-1]

For purposes of Web-content records, Web content is limited to what is accessed over HTTP. All other transfer protocols (i.e., FTP and SMTP) are excluded. [<http://www.archives.gov/records-mgmt/initiatives/web-content-records.html>, accessed June 9, 2006]

Hypertext Transfer Protocol-Secure

The protocol for accessing a secure Web server. The use of HTTPS in the URL directs the message to a secure port address instead of the default Web port address of 80. [Section II of glossary, DA PAM 25-1-1]

Hyperlink

A link in a given document to information within another document. These links are usually represented by highlighted words or images. The user also has the option to underline these hyperlinks.

Hypermedia

Richly formatted documents containing a variety of information types, such as textual, image, movie, and audio. These information types are easily found through hyperlinks.



Image or imagery

Still or moving pictorial representation of a person, place, thing, idea, or concept, either real or abstract, used to convey information. May be chemically, digitally, or manually produced. [Paragraph 7-7b(1)(a) and Section II of glossary, AR 25-1]

Indicator

Data derived from friendly detectable actions and open-source information that adversaries can interpret and piece together to reach conclusions or estimates of critical or classified information concerning friendly intentions, capabilities, or activities. [Glossary, DoD 5205.02-M]

Individual

A living citizen of the United States or an alien lawfully admitted for permanent residence. The parent of a minor or the legal guardian of any individual also may act on behalf of an individual. Members of the U.S. armed forces are “individuals.” Corporations, partnerships, sole proprietorships, professional groups, businesses, whether incorporated or unincorporated, and other commercial entities are not “individuals” when acting in an entrepreneurial capacity with DoD, but persons employed by such organizations or entities are “individuals” when acting in a personal capacity (e.g., security clearances, entitlement to DoD privileges or benefits). [Enclosure 2 (definitions), DoDD 5400.11; Section II of glossary, AR 340-21]

Information

Any communication or representation of knowledge such as facts, data, or instructions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. Information can have a different meaning for different people, as information is the meaning a human assigns to data by means of the known conventions used in their representation (see JP 1-02). The same information may convey different messages to different recipients and thereby provide “mixed signals” to information gatherers and users. Information is a shared resource and is not owned by any organization within the restrictions of security, sensitivity, and proprietary rights. [Glossary, DoDD 5230.9; Section 3, Chapter 1, and Part II of glossary, JP 3-13; Section II of glossary, AR 25-1; glossary, FM 3-13]

This definition includes information that a DoD organization disseminates from a Webpage, but does not include the provision of hyperlinks to information that others disseminate. This definition also does not include opinions, where the component’s presentation makes it clear that what is being offered is someone’s opinion rather than fact or the component’s views. [Paragraph 4, Attachment 2, memorandum from the DEPSECDEF, “Ensuring Quality of Information Disseminated to the Public by the Department of Defense”]

Any knowledge that may be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of, DoD. [Paragraph 3, DoDD 5200.1]

Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. [Definitions section, DoDD 5230.09; g lossary, DoDD 8000.01]

Information assurance

The protection of systems and information in storage, processing, or transit from unauthorized access or modification; denial of service to unauthorized users; or the provision of service to authorized users. It also includes those measures necessary to detect, document, and counter such threats. IA is the security discipline that encompasses COMSEC, INFOSEC, and control of compromising emanations. [Section II of glossary, AR 530-1]

Ensures the availability, integrity, identification, authentication, confidentiality, and non-repudiation of friendly information (information processed by the Army’s information-based systems), and forbids the access to the information and systems by hostile forces. As a subset of defensive IO, IA includes provisions for protection,

detection, and response capabilities. The protection capability is composed of devices that ensure emission security, COMSEC, COMPUSEC, and INFOSEC. Detection is the capability to determine abnormalities such as attacks, damages, and unauthorized modifications in the network via mechanisms such as intrusion-detection systems. The response capability refers to the ability to restore normal operations as well as the ability to respond to a detected entity. [Section II of glossary, DA PAM 25-1-1]

The means to ensure the confidentiality, integrity, availability, authentication, verification, protection, and non-repudiation of information processed by Army ISs. IA provides a measure of confidence that the security features, practices, procedures, and architectures of an IS accurately mediate and enforces the security policy. IA recognizes that interconnected systems create shared risks and vulnerabilities where an intruder only has to penetrate the weakest link to exploit the entire network. The value of information must be measured in terms of how critical it is to the authentication and integrity of the data and is as important as the confidentiality of that information. IA includes security of information and related systems, C2, physical, software, hardware, procedural, personnel, network, COMSEC, operations, intelligence, and risk assessment (including Web risk assessment). IA enhances effective C2 of friendly forces by protecting critical information infrastructures from unauthorized users, detecting attempts to obtain or alter information, and reacting to unauthorized attempts to obtain access to or change information. These measures focus on the integrity, confidentiality, availability, authentication, verification, protection, and non-repudiation of the infrastructures and the information contained within. [Paragraphs 5-1 and 5-1c, AR 25-1; Section II of glossary, DA PAM 25-1-1]

Information clearance

See *clearance of information* entry.

Information-dissemination product

Any book, paper, map, machine-readable material, audiovisual production, or other documentary material, regardless of physical form or characteristic, that a component disseminates to the public. This definition includes any electronic document, CD-ROM, or Webpage. [Paragraph 6, Attachment 2, memorandum from the DEPSECDEF, "Ensuring Quality of Information Disseminated to the Public by the Department of Defense"]

Information lifecycle

The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition. [Glossary, DoDD 8000.01]

Information technology

Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the federal government. IT includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources, but does not include any equipment that is acquired by a federal contractor incidental to a federal contract. (Reference 40 USC Subtitle III (Clinger-Cohen Act of 1996).) [Glossary, DoDD 8000.01; Paragraph 1-6b and Section II of glossary, AR 25-1]

The hardware, firmware, and software used as a part of an information system to perform DoD information functions. This definition includes computers, telecommunications, automated information systems, and automatic data-processing equipment. IT includes any assembly of hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information. [Section II of glossary, AR 25-2]

Integrity

Standard of the QI Program. Assurance of (and the degree of that assurance) security of / protection of information from unauthorized (intentional or unintentional) access or revision, to ensure that the information is not compromised through corruption or falsification. [Section II of glossary, AR 25-1; Section II of glossary, AR 25-2; Paragraph 7, Attachment 2, memorandum from the DEPSECDEF, "Ensuring Quality of Information Disseminated to the Public by the Department of Defense"]

The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed. [Section II of glossary, AR 380-5]

Internet

An electronic communications network that connects computer networks and organizational computer facilities in government, academic, and business institutions around the world. [Section II of glossary, AR 25-1; Section II of glossary, DA PAM 25-1-1]

The loosely connected worldwide collection of computer systems that uses a common set of communications standards to send and receive electronic information. [Part III, DoD Web policy]

The global collaboration of data networks that are connected to each other, using common protocols (for example, TCP / IP) to provide instant access to the information from other computers around the world. [Section II of glossary, AR 25-2; Section II of glossary, AR 530-1]

Internet Protocol

A DoD standard protocol designed for use in interconnected systems of packet-switched computer communication networks. The IP provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed-length addresses. The IP also provides for fragmentation and reassembly of long datagrams, if necessary, for transmission through small-packet networks. [Section II of glossary, DA PAM 25-1-1]

Intranet

A computer network that functions like the Internet, using Internet-standard Web-browser software to access and process the information that employees need, and is located on computers within the organization / enterprise. A firewall is usually used to block access from outside the intranet. Intranets are private Websites, accessible only by the organization's employees or others with authorization. [Section II of glossary, AR 25-1; Section II of glossary, AR 25-2]

An information utility that makes organizational and departmental information accessible via the standards of the Internet: email (SMTP), WWW, FTP, and other Internet services. [Section II of glossary, AR 25-1]



Knowledge management

An integrated approach to identify, manage, and share all an organization's information assets, including management information systems (databases, documents, policies, and procedures) learning processes and personnel expertise, to fulfill organizational objectives. [Section II of glossary, AR 5-1]



LinkedIn

A professional on-line community used to network with fellow professionals; an on-line resume-sharing site.

Long-term record

The designation applied to records that have value beyond the business process, such as for historical, lessons learned, or research purposes. This type of record is kept longer than six years. [Section II of glossary, TR 25-1]



Metadata

Information describing the characteristics of data; data or information about data; descriptive information about an organization's data, data activities, systems, and holdings. Refers not only to the set of definitions of the data in a data asset, but also to its formats, processing, transformations, and routing from source to target information system. Everything except the data's content constitutes metadata. Metadata allow for content management. Metadata foster knowledge of the content, the environment within which content resides, the interrelationship among content

environments, and the ability for content to evolve. A metatag is an HTML tag containing metadata. [Section II of glossary, AR 25-1; Paragraph 5-2f, DA PAM 25-1-1]

Mission-related

Processes and functions that are closely related to the mission. (For example, the mission of “direct and resource the force” has the mission-related functions of planning, programming, policy development, and allocating of resources.) [Section II of glossary, AR 25-1]

Multimedia / VI productions

Pertaining to the processing and integrated presentation of information in more than one form, for example, video, voice, music, or data. [Section II of glossary, DA PAM 25-1-1]

The synchronized use of two or more types of media, regardless of the delivery medium. [Section II of glossary, AR 25-1]

Multimedia / VI productions are a combination of motion media with sound in a self-contained complete presentation, developed according to a plan or script for conveying information to, or communicating with, an audience. The delivery of multimedia / VI productions includes, but is not limited to, solid-state memory cards, hard disk, removable magnetic or optical disk, digital videodisc (DVD), and the Internet. Multimedia / VI productions are usually displayed electronically or optically. Multimedia productions may include combinations of text, and/or other VI products such as motion video, graphics, still photography, animation, or audio. Multimedia / VI productions include informational products (for example, recruiting, public, or command information) or electronic publications. Multimedia / VI productions are of two types: local productions and non-local productions. Local productions support the needs of a local installation and its area of responsibility with no dissemination of the production outside the area. Non-local productions are for multi-installation, FOA, Army, or DoD-wide use. [Paragraphs 7-7a(1), (2), and (6), AR 25-1]

MySpace

A site where people can meet others with similar interests, creating on-line communities by sharing videos, photos, and personal information.



National-security information

Possibly classified information, but also includes CUI, which includes FOUO and SBU. *National security* is defined as the national defense or foreign relations of the United States.⁶⁰² *Classified national security information*, or *classified information*, is defined as information and / or material that has been determined, pursuant to EO 12958 or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary or readable form. (See CUI and FOUO definitions above.) SBU is a DoS designation which warrants a degree of protection and administrative control, and meets the criteria for exemption from mandatory public disclosure under the FOIA. When SBU information is included in DoD documents, the documents will be marked as if the information is FOUO. [Paragraphs 1-1, 5-7 and 5-8, and Section II of glossary, AR 380-5] See Appendix B, AR 380-5, for the text of EO 12958. See the OPSEC reviewer’s checklist in Chapter 4 for categories of national security information. (**Note:** A 2008 White House decision⁶⁰³ determined that the entire federal government would use *CUI* and not *SBU* – this change should be reflected in the next version of AR 380-5. This definition uses terminology in the current AR 380-5.)

Classifications are: *confidential*, if the information could reasonably be expected to cause damage to the national security if unauthorized disclosure occurs; *secret*, if the information would cause serious damage to the national security; and *top secret*, if the information would cause exceptionally grave damage. [Section II of glossary, AR 380-5]

⁶⁰² Paragraph 3.3, DoDD 5200.1.

⁶⁰³ Memorandum for heads of executive departments and agencies, “Designation and Sharing of Controlled Unclassified Information,” May 9, 2008.

National-security system (44 USC 3542)

Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function, operation or use of which:

- Involves intelligence activities;
- Involves cryptologic activities related to national security;
- Involves C2 of military forces;
- Involves equipment that is an integral part of a weapon or weapons system; or
- Is critical to the direct fulfillment of military or intelligence missions,

but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel-management applications). An NSS is also a system that is protected at all times by procedures established for information that has been specifically authorized under criteria established by an executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy.

[Glossary, DoDD 8000.01; Section II of glossary, AR 25-2]

Net-centric

Relating to or representing the attributes of a robust, globally interconnected network environment (including infrastructure, systems, processes, and people) in which data are shared timely and seamlessly among users, applications, and platforms. [Glossary, DoDD 8000.01]

News clip

A news story of an event recorded and released on motion picture or videotape for viewing by an internal Army audience or the general public. [Section II of glossary, AR 25-1]

Non-public data / information

Data / information that is personally identifiable and subject to the Privacy Act, classified according to the National Security Act, subject to a FOIA exemption, or sensitive. [Section II of glossary, AR 25-1]

Non-public-domain content

Information and the data from which information is derived are broadly categorized as public domain and non-public domain. Non-public data or information is defined as personally identifiable and subject to the Privacy Act, classified according to the National Security Act, subject to a FOIA exemption, or sensitive. Unclassified FOIA-exempt information or data is non-public and designated FOUO. Non-public information or data may be shared for official purposes within the Army, subject to any stipulated access and release restrictions. Non-public Army data in this category may be made available to authorized individuals via the AKO portal or other controlled-access (private) Web servers, as required. Requests for non-public data from private individuals / organizations should be coordinated with/referred to the local FOIA/Privacy Act official for determination of whether or not the data are releasable. [Paragraph 1-7b and Section II of glossary, AR 25-1]

Non-public Website

Same as private Website; Army Website with access restricted by password or PKI user authorization. [Section II of glossary, AR 25-1]

Non-releasable information

Any official information that is generally not available to the public and which would not be released under the FOIA. Information prohibited from public release. [Paragraph 13-14d(6), AR 360-1]



Objectivity

Standard of the QI Program. Involves two distinct elements: presentation and substance. Includes whether disseminated information is being presented in an accurate, clear, complete, and unbiased manner. The information must also be presented in the proper context. Sometimes, in disseminating certain types of information to the public, other information must also be disseminated to ensure an accurate, clear, complete, and unbiased presentation. Also,

the component must identify the sources of the disseminated information (to the extent possible, consistent with confidentiality protections) and, in a scientific, financial, or statistical context, the supporting data and models, so that the public can assess for itself whether there may be some reason to question the objectivity of the sources. Where appropriate, supporting data (including classified data) should have full, accurate, transparent documentation, and error sources affecting data quality should be identified and disclosed to users when possible. In addition, “objectivity” involves ensuring accurate and reliable information, including classified information. In a scientific, financial or statistical context, the original and supporting data shall be generated, and the analytical results shall be developed, using sound statistical and research methods.

If the data and analytical results have been subjected to formal, independent, external peer review, the information can generally be considered of acceptable objectivity. However, this presumption is rebuttable based on persuasive showing by the petitioner in a particular instance.

In those situations involving dissemination of influential scientific, financial, or statistical information, a high degree of transparency of data and methods must be ensured to facilitate the reproducibility of such information by qualified third parties.

Components shall not require that all disseminated original and supporting data be subjected to the reproducibility requirement. Components may identify those particular types of data that can be practicably be subjected to the reproducibility requirement, given ethical, feasibility, or confidentiality constraints.

Making the data and models publicly available will assist in determining whether analytical results are capable of being substantially reproduced. However, these guidelines do not alter the otherwise applicable standards and procedures for determining when and how information is disclosed. Thus the objectivity standard does not override other compelling interests such as privacy, trade secret, intellectual property, and other confidentiality protections such as security classifications. [Paragraph 8, Attachment 2, memorandum from the DEPSECDEF, “Ensuring Quality of Information Disseminated to the Public by the Department of Defense”]

Official command spokesperson

Commander, or someone designated by the commander to speak for him or her; a person who frequently interacts with the public by nature of his / her position and duties. An official command spokesperson *may* be a GO, SES, or PAO, but *must* be a government official, either a Soldier or Army civilian. [Section II of glossary, AR 360-1]

Official imagery

All photographic and video images, regardless of the medium in which they are acquired, stored, or displayed, that are recorded or produced by persons acting for or on behalf of DoD activities, functions, or missions. [Paragraph 3, DoDI 5040.5. Also, Paragraph 13-4, AR 360-1]

Official information

All information that is in DoD’s custody and control, relates to information in DoD’s custody and control, or was acquired by DoD employees as part of their official duties or because of their official status. [Glossary, DoDD 5230.9, Paragraph 13-14d, AR 360-1]

Official record

Includes all documentary materials, regardless of physical form or characteristics, that provide evidentiary accounting for decisions, policies, plans, organizations, functions, procedures, operations, and essential transactions of an organization as defined in 44 USC 3301. [Section II of glossary, TR 25-1]

The product(s) of data compilation, such as all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the U.S. government under federal law in connection with the transaction of public business, and in DoD’s possession and control. [Paragraph 1-402, AR 25-55]

Any item, collection, or grouping of information about an individual. [Section II of glossary, AR 340-21]

Official statement

Statement on Army matters by an Army representative acting in an official capacity. [Section II of glossary, AR 360-1]

Official Website

A DoD Website that is developed and maintained with command sponsorship and approval, and for which the DoD component, a subordinate organization, or individual exercises editorial control over content. The content of official DoD Websites is of an official nature that may be endorsed as the official position of the DoD component. Content may include official news releases, installation history, command position papers, etc. Official DoD Websites are prohibited from displaying sponsorships or commercial advertisements. [Part III, DoD Website policy; Paragraph 13-14d, AR 360-1] Policy / guidance applies to unclassified DoD Websites regardless of domain (.com, .edu, .org, .mil, .gov) or sponsoring organization. Army Websites must comply with procedures published in AR 25-1, Paragraph 6-7.

An official Army Website is not limited to the army.mil domain, as Websites published and sponsored by Army commands but hosted on commercial servers (servers other than army.mil – i.e., .com) are considered official sites and are subject to AR 25-1, Paragraph 6-7, and other policies / guidance. AWRAC reviews Army Websites on the dot-mil, and all other domains used for communicating official information, to ensure they are compliant with DoD and Army policies and best practices.

Operations security

For DoD components, OPSEC is a process of identifying critical information and then analyzing friendly actions attendant to military operations, defense acquisition, defense activities, and other sensitive activities to 1) identify actions that can be observed by adversary intelligence systems; 2) determine what indicators might be obtained by hostile intelligence systems that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and 3) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. [Enclosure 2, DoDD 5205.2; Part III, DoD Web policy; CJCSI 3213.01C; Part II of glossary, JP 3-13; executive summary, Paragraph 2, Chapter I, and Part II of glossary, JP 3-54; Section II of glossary, AR 25-2; Chapter 3 and glossary, FM 3-13; Section II of glossary, AR 530-1]

The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with the planning and conducting of military operations and other activities. [Section II of glossary, AR 380-5]

OPSEC compromise

The disclosure of critical information or sensitive information which has been identified by the command and any higher headquarters that jeopardizes the unit's ability to execute its mission or to adequately protect its personnel and/or equipment. [Section II of glossary, AR 530-1]

Critical or sensitive information that has been compromised and is available in open sources and the public domain should not be highlighted or referenced publicly outside of intra-governmental or authorized official communications because these actions provide further unnecessary exposure of the compromised information. [Paragraph 1-5d, AR 530-1]

OPSEC indicators

Those elements of an action or piece of information that make it potentially useful to an adversary. Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information regarding friendly intentions, capabilities, or activities that enables the adversary to reach personal conclusions or official estimates. Examples of OPSEC indicators are found at Appendix H; however, do not use this as a checklist, since each operation or activity will have indicators unique to itself. [Enclosure 2, DoDD 5205.2; CJCSI 3213.01C; Paragraph 1c, Chapter III, Paragraph 2, Appendix C, and Part II of glossary, JP 3-54; Appendix D and Section II of glossary, AR 530-1; Chapter 3 and glossary, FM 3-13]

OPSEC vulnerability

A type of hazard related to the EEFI. [Paragraph 3-24, Chapter 3, FM 3-13]

A condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision-making. Vulnerabilities can be identified by answering these questions: 1) What indicators (friendly actions and open-source information) of critical information not known to the adversary will be created by the friendly activities that will result from the planned operation? 2) What indicators can the adversary actually collect? 3) What indicators will the adversary be able to use to the disadvantage of friendly forces? (Can the adversary analyze the information, make a decision, and take appropriate

action in time to interfere with friendly planned operations?) [Paragraphs 1c and 2c, Chapter III, and Part II of glossary, JP 3-54; Section II of glossary, AR 530-1; Chapter 3 and glossary, FM 3-13]

Organizational self-assessment

A framework that allows Army organizations to measure how well they are meeting their stated goals and customer needs, and that provides a systematic approach for gathering the information and insight required to make informed management decisions. [Section II of glossary, AR 5-1]



Permanent record

Information that has been determined by the archivist of the United States to have enough value to warrant its preservation by NARA for the life of the United States. The AASA is the archivist of the Army, per DA General Order 2006-01, and coordinates permanent records with the archivist of the United States, but performance of records-management missions and functions remain under oversight of the CIO / G-6. [Section II of glossary, AR 25-1; Section II of glossary, TR 25-1]

Persistent cookies

Cookies that can be used to track users over time and across different Websites to collect personal information. [Section II of glossary, AR 25-1]

Personal information / personally identifying information

Personal information (AR 340-21 term) is information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., SSN; age; military rank; civilian grade; marital status; race; salary; home or office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc). (See Appendix J.) Such information also is known as *personally identifiable information*, defined as information which can be used to *distinguish* or *trace* an individual's identity, such as his or her name; SSN; date and place of birth; mother's maiden name; and biometric records, including any other personal information which is linked or linkable to a specified individual). [Enclosure 2 (definitions), DoDD 5400.11]

Information about an individual that is intimate or private to the individual, as distinguished from information related solely to the individual's official functions or public life. [Section II of glossary, AR 340-21]

PII includes, but is not limited to, name, rank, unit or other location information, email address, home postal address, home telephone number, SSN, date of birth, or any other identifying information about all DoD personnel, including civilians, active-duty military, military family members, contractors, members of the National Guard and Reserves, and Coast Guard personnel when the Coast Guard is operating as a service in the Navy. Prohibited PII also includes family information in a permitted biography (that of a command spokesperson), the biography of a non-command spokesperson, or lists / rosters of names of people. [Part III, DoD Website policy; Paragraph 13-14d, AR 360-1]

Podcast

On-line audio that can be downloaded to devices such as PCs or handheld devices (wireless phones, MP3 players, iPods). These can be subscription based or free, single-use, or repeated-use content.

Portable electronic device

Portable IS or device with or without the capability of wireless or local-area-network connectivity. PEDs include, but are not limited to, cellphones, pagers, PDAs (for example, Palm Pilots and Pocket PCs), laptops, memory sticks, thumb drives, and two-way radios. Current technologies (infrared, radio frequency, voice, video, microwave) allow the inclusion of many capabilities within a single device. From a security perspective, PEDs' capabilities dramatically increase the risks associated with IS and network access, so PEDs must support PKI, digital certificates, FIPS, or NSA-validated cryptomodules or data-encryption standards appropriate for the classification level of the information processed. [Paragraph 4-29, AR 25-2]

Positive security and access control

Control that authenticates individual client / user access. The Army IA policy regarding access controls is to require a minimum of user ID and an authenticator.

Privacy Act of 1974

The public law, amending title 5 USC 552 and adding section 552a. The intent of this law is to safeguard individual privacy from misuse of personal information in federal records. DoDD 5400.11 and AR 340-21 implement the law. [Section II of glossary, AR 360-1]

Private Webserver

A Webserver that is designed for and / or provides information resources that are limited to a particular audience (i.e., DoD) or a subset thereof. (This includes Webservers that provide interfaces to email systems.) A private Webserver restricts, or attempts to restrict, general public access to it. Although once considered common means of restriction (thereby making the information private), the use of domain restriction (e.g., .mil and/or .gov) and filtering of specific IP addresses makes the content publicly accessible; only positive access control such as unique user ID and/or password authentication, encryption (i.e., DoD certificates), and physical isolation make the server private. Any DoD-operated Webserver that provides *any* information resources that are not intended for the general public shall be considered a private Webserver and is subject to the policy for private servers. [From attachment in memorandum from the ASD-C3I, "Public Key Enabling (PKE) of Applications, Webservers and Networks for the Department of Defense (DoD)"; attachment in memorandum from ASD-C3I, "Department of Defense (DoD) Public Key Infrastructure (PKI)"]

Private Website

A Website that screens or challenges users prior to permitting access to the information posted on the site. Private Websites may be connected to an intranet (that is, users are screened from accessing the entire network) or the Internet (that is, users are screened before entry into the specific Website). The term *Website* also includes any network service that gives a persistent presence to information on the Internet, with or without an HTTP front end (for example, FTP site). [Section II of glossary, TR 25-1]

(Note: For purposes of content review, the unrestricted-content area of AKO (accessible to all accounts) will be reviewed just as if generally publicly accessible, although AKO uses access control. According to the VAD, 1st IOC, AKO unrestricted areas are not sufficiently secure; AKO is insufficient for FOUO access IAW DoD policy because of the types of people who have access: Army retired, medical retired, U.S. Military Academy (USMA) cadets, ROTC cadets (MS III and IV), DA civilians, non-appropriated fund civilians, and, as guest accounts, medically discharged personnel, local national employees, DoD civilians, Army volunteers, contractors, retired DA civilians, family members of "full" AKO member, foreign officers attached to the U.S. Army, initial-entry Soldiers, ROTC cadets (MS I and II), U.S. Air Force, U.S. Coast Guard, U.S. Marine Corps, U.S. Navy, Department of Homeland Security employees, and federal civilian agencies. As AKO and DKO integrate, the accounts categories will, of course, change. VAD 1st IOC states that it cannot "recommend specific technical architectures for each site for FOUO material, but some organizations do post their information to AKO (https://www.us.army.mil/portal/portal_home.jhtml) and list the material in a [knowledge center] or use AKO as the 'authenticator' as depicted in the U.S. Army Information Assurance Webpage (<https://informationassurance.us.army.mil/SpecialContent.asp?special=iaomain>). However, basic AKO authentication by itself is insufficient for posting FOUO information, because AKO accounts can be held by individuals not authorized FOUO access. If FOUO is to be posted on AKO (or one of its 'subsites'), additional/secondary checks of user 'credentials' are required to ensure appropriate user authentication – and may require entry of additional password/id.")

Proprietary format

Software or Web-application format developed, licensed, and / or sold by a commercial firm for profit. Proprietary formats often do not have universality.

Proxy server

A server acting on behalf of another server or servers. Such an arrangement allows a single point of entry or exit into a TCP / IP network. A proxy server may also have built-in software that will allow it to be configured to act as a firewall, cache server, or logging server. [Section II of glossary, AR 25-2]

Public Affairs

Public information, command information, and community-engagement activities directed toward both external and internal publics with interest in DoD. Public Affairs activities contribute to U.S. government strategic

communication and DoD objectives by communicating information about military activities to domestic, international, and internal audiences. As a function of command, PA is an operational capability vital to meeting DoD public information and communications requirements. [Glossary, DoDI 5400.13]

Public affairs

Matters of general interest or concern to the public – especially those dealing with social or political issues. See also *Army Public Affairs*. [Section II of glossary, AR 360-1]

Public Affairs Office(r)

The entity consisting of public-information, command-information, and community-relations activities directed toward both the external and internal publics with interest in DoD. An individual officially designated to perform Army Public Affairs activities. [Section II of glossary, JP 3-13; glossary, FM 3-13]

Publicly accessible Website (or public Website)

Army Website with access unrestricted by password or PKI user authorization. *Public* refers to the at-large audience on the Internet; anyone who can access a Website through a browser. [Section II of glossary, AR 25-1; Section II of the glossary, AR 530-1; Paragraph 5B, ALARACT message, “Website Security Policy Compliance,” Dec. 19, 2008]

A Website that is accessible from the Internet and use no positive access control, for example, user authentication or firewalls, to restrict access to the information posted on the Website. *Website* is used to also include any network service that gives a persistent presence to information on the Internet, with or without an HTTP front end (for example, FTP site). [Section II of glossary, TR 25-1]

Access is not limited. Includes Websites and other information technologies that have very limited access controls, such as domain and / or IP address restrictions. [Enclosure 3, DoDI 8410.1]

The collection of Internet media, services, supporting technology and systems, available without access controls to an unlimited audience at URL; a Web address that begins with a protocol indicator (e.g., http://, https:// and ftp://). Publicly accessible Websites should not contain mission data but may contain mission-related data if the Website mission is to inform the public. [Glossary, DoDI 5400.13]

Public-domain information

Unclassified information that does not qualify for the status of CUI, and is deemed to be actually or potentially suitable for disclosure to the public at large. All U.S. Army information must be reviewed prior to release to the public. The proponent for disclosure of U.S. Army public-domain information is the Public Affairs Office. [Paragraph 2-3b(2), AR 380-10]

Information that is not exempt under provisions of the FOIA is considered to be in the public domain. [Paragraph 1-505, AR 25-55]

Information and the data from which information is derived are broadly categorized as public domain and non-public domain. Public-domain data or information is government-owned and is not personally identifiable, classified, or otherwise subject to a FOIA or Privacy Act exemption, or otherwise considered to be sensitive under AR 25-2. It is either routinely made available to the public, or provided upon public request, with or without charge. Public-domain Army data may be made available to the public via the Army homepage or other authorized Army public Website. [Paragraph 1-7b, AR 25-1]

Public-domain information on each TRADOC organization’s Website will include a brief description of the organization’s functions and missions, a brief description of any sub-sections, and the required links and pages outlined in this *Guide*.

Public information

The ability to disseminate truthful, timely, accurate, culturally attuned information about military activities, consistent with security guidelines, to local, national, and international audiences. [Glossary, DoDI 5400.13]

Public Key Infrastructure

The framework and services that provide the generation, production, distribution, control, tracking, and destruction of public key certificates. [Attachment, memorandum from ASD-C3I, “Public Key Enabling (PKE) of Applications, Webservers and Networks for the Department of Defense (DoD)”]

Public Key Infrastructure certificate

A digital representation of information that binds the user’s identification with the user’s public key in a trusted manner. At a minimum, this information (1) identifies the certification authority using it, (2) names or identifies its user, (3) contains the user’s public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [Attachment in memorandum from ASD-C3I, “Department of Defense (DoD) Public Key Infrastructure (PKI)”]



Quality

An encompassing term comprising utility, objectivity, and integrity. Therefore, the QI Program guidelines sometimes refer to these statutory terms collectively as “quality.” [Paragraph 9, Attachment 2, memorandum from the DEPSECDEF, “Ensuring Quality of Information Disseminated to the Public by the Department of Defense”]



Record

All books, papers, maps, photographs, machine-readable items (such as disks, tapes, cards, printouts, aperture cards, roll microfilm, microfiche, laser disk, optical disk, optical card, other optical recording media, film slides, transparencies, or other documentary materials, regardless of physical form or characteristics) made or received by any DA entity as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities because of the informational value of the data. [Section II of glossary, AR 25-1]

In another sense, a *record* or *system of records* is any item, collection, or grouping of information, whatever the storage media (for example, paper or electronic), about an individual that is maintained by a DoD component – including, but not limited to, an individual’s home address, home telephone number, SSN, education, financial transactions, medical history, and criminal or employment history – and that contains his or her name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint, voiceprint, or photograph. [Enclosure 2 (definitions), DoDD 5400.11, and Section II of glossary, AR 340-21]

Release of information

Dissemination of information to the public, either on Army initiative or in response to an external request. Includes written news releases, still photographs, motion-picture films, question-and-answer interviews, speeches, audio or videotape recordings, articles for publication in printed media or for broadcast by radio or television, and oral responses to queries. [Section II of glossary, AR 360-1]

Reproducibility

The information is capable of being substantially reproduced, subject to an acceptable degree of imprecision. For information judged to have more/less important impacts, the degree of imprecision that is tolerated is reduced / increased. If components apply the reproducibility test to specific types of original and supporting data, standards for replication of laboratory data shall be established. With respect to analytic results, *capable of being substantially reproduced* means that independent analysis of the original or supporting data using identical methods would general similar analytic results, subject to an acceptable degree of imprecision or error. [Paragraph 10, Attachment 2, memorandum from the DEPSECDEF, “Ensuring Quality of Information Disseminated to the Public by the Department of Defense”]

Review for clearance

The process by which information that is proposed for public release is examined for compliance with established national and DoD policies and to determine that it contains no classified or export-controlled information. Although DoDD 5230.9 states that release of information to the public, cleared by the OSR, is the responsibility of the

originating office, the proponent for public-domain information is the PAO, so coordination with / clearance by PAO is a requirement. [Definitions section, DoDD 5230.9]

Risk

The probability that a particular threat will exploit a particular vulnerability of an information system or telecommunications system. [Section II of glossary, AR 25-2]

Risk assessment

Process of analyzing threats to and vulnerabilities of an information system, and determining potential adverse effects that the loss of information or capabilities of a system would have on national security and using the analysis as a basis for identifying appropriate and cost-effective countermeasures. [Section II of glossary, AR 25-2]

Routine use

Disclosure of a record outside DoD without the consent of the subject individual for a use that is compatible with the purpose for which the information was collected and maintained by DA. The routine use must be included in the published system notice for the system of records involved. [Section II of glossary, AR 340-21]



Safeguarded information

Defense information requiring protection under DoDD 5200.1 and AR 380-5, or information protected or controlled under AR 20-1, or information controlled under DoDD 5230.24 and DoDD 5230.25. [Section II of glossary, AR 360-1]

Scientific and technical material

Material that has limited interest within a specialized field or to a specific audience because of its subject matter and/or the technical or scientific language in which the material is presented. [Section II of glossary, AR 360-1]

Secure Sockets Layer

A data-transport protocol that works by combining programs and encryption / decryption routines existing on the Web hosting computer and in the user's browser. Therefore SSL only authenticates the server, while the client / user remains unauthenticated. HTTPS, which some military Websites use as pseudo-security, is publicly accessible; the "s" at the end of HTTP merely means that a Website visitor has established an SSL session through the HTTPS-secured URL.

Selective benefit

Army support to any person; group or corporation, whether profit or non-profit; religion, sect, religious or sectarian group, or quasi-religious or ideological movement; fraternal organization; political organization; or commercial venture that the Army would not provide if available under similar conditions to other such entities upon request. [Section II of glossary, AR 360-1]

Senior commander

The senior commander is normally, though not always, the senior general officer at the installation. Within TRADOC, he / she is often dual-hatted as the mission (such as the TRADOC CoE) commander and the senior commander. As senior commander, his / her mission is the care of Soldiers, families and civilians, and to enable unit readiness – his / her responsibilities are installation-focused. The senior commander is the SecArmy's / CSA's representative at the installation and is the installation commander. (As mission commander, his / her responsibilities are, of course, mission-focused.) The senior commander can, in rare cases, be an HQ DA-appointed civil servant vs. a uniformed senior commander; he / she assumes the senior commander roles and responsibilities except UCMJ and command authority, and is called the senior manager vs. senior commander. Where the mission commander and senior commander are not dual-hatted, the senior commander assumes the duties and responsibilities of the senior mission commander where that title is mentioned in Army regulations, except for regulations involving operational duties and responsibilities – mission commanders retain operational duties and responsibilities. The senior commander serves as the senior Army representative to the surrounding community. [Paragraph 2-5, AR 600-20]

Senior commander's public affairs office(r)

See definition for command / activity PAO.

Sensitive information

Information requiring special protection from disclosure that could cause compromise or threat to our national security, an Army organization, activity, family member, DA civilian, or DoD contractor. Sensitive information refers to unclassified information, while sensitive compartmented information (SCI) refers to classified information. Appendix I includes examples which may be deemed sensitive; however, sensitive information is not limited to this list. For instance, examples of sensitive unclassified information given in the SECDEF message, "Website OPSEC Discrepancies," are CONOPs, OPLANs, and SOPs. [Section II of glossary, AR 530-1]

Any information the loss, misuse, or unauthorized access to, or modification of, which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, USC (The Privacy Act), but which has not been specifically authorized under criteria established by executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy. Sensitive information includes the following categories:

- FOUO – IAW DoDD 5400.7-R, information that may be withheld from mandatory public disclosure under the FOIA;
- Unclassified technical data – data related to military or dual-use technology that is subject to approval, licenses, or authorization under the Arms Export Control Act and withheld from public disclosure IAW DoD 5230.25;
- DoS' SBU – information originating from DoS that has been determined to be SBU under appropriate DoS INFOSEC policies;
- Foreign government information – information originating from a foreign government that is not classified *confidential* or higher but must be protected IAW DoD 5200.1-R;
- Privacy data – personal and private information (for example, individual medical information, home address and telephone number, SSN) as defined in the Privacy Act. This includes information in routine DoD payroll, finance, logistics, and personnel-management records;
- Special-handling data; and
- CUI.

[Computer Security Act of 1987; Paragraph 5-19, AR 380-5; Section II of glossary in AR 25-2; Paragraph 1-5c, AR 530-1. Also, TR 25-1. AR 380-5 notes that two aspects of this definition of "sensitive" information, based on the Computer Security Act, deserve attention: this act applies only to unclassified information which deserves protection, and second, unlike most other programs for protection of information, the act is concerned with protecting the availability and integrity, as well as the confidentiality, of information. Much of the information which fits the act's definition of *sensitive* falls within the other categories of information discussed in Chapter 5, AR 380-5.]

Server

A program that awaits and fulfills requests from client programs on the same or other computers. On the Web, servers are the location of most Web content. The server may be a complex system of multiple tiers of applications that all interact via configurations that are specific to that computer. [Glossary, <http://www.archives.gov/records-mgmt/initiatives/web-content-records.html>, accessed June 9, 2006]

Short-term record

The designation applied to records that have no value beyond the business process and usually not kept longer than six years. [Section II of glossary, TR 25-1]

Social engineering

Term used among crackers and security professionals for cracking techniques that rely on weaknesses in process rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system's security. Classic scams include phoning up a user or helpdesk who has the required information and posing as a field-service tech or a fellow employee with an urgent access problem. [Section II of glossary, AR 25-2]

Social media

An umbrella term that defines various activities that integrate technology, social interaction, and the construction of words and pictures. This interaction, and the manner in which information is presented, depends on the varied perspectives and shared meaning as people share their stories and understandings. Social media use the “wisdom of crowds” to connect information in a collaborative manner. Social media can take many different forms, including Internet forums, message boards, blogs, wikis, podcasts, pictures, and video. Examples of social-media applications are Google (reference, social networking), Wikipedia (reference), MySpace (social networking), Facebook (social networking), Last.fm (personal music), YouTube (social networking and video sharing), Second Life (virtual reality), and Flickr (photo sharing). Social media, or social networking (one example of social media), has a number of characteristics that make it fundamentally different from traditional media such as newspapers, television, books, and radio. Primarily, social media depends on interactions between people as the discussion and integration of words build shared meaning, using technology as a conduit. Social media is typically available via feeds, enabling users to subscribe via feed readers. [http://en.wikipedia.org/wiki/Social_media]

Social-networking sites

On-line networking platforms that allow registered users to interact with other users for social or professional purposes. Examples include MySpace, Facebook, and LinkedIn.

Stakeholders

Includes all groups that might be affected by an organization's actions and success. Examples of key stakeholders include leaders, customers, employees, partners, and local or professional communities. [Section II of glossary, AR 5-1]

Still photography

The medium used to record still imagery; includes negative and positive images. [Section II of glossary, AR 25-1]

Strategic plan

The document produced by the process by which an organization envisions its future and develops special management strategies and action or implementation plans to achieve that future. [Section II of glossary, AR 5-1]

Strategic planning

A continuous and systematic process whereby guiding members of an organization make decisions about its future, develop the necessary procedures and operations to achieve that future, and determine how success is to be measured. [Section II of glossary, AR 25-1]

Substantive

Having the character of an independent, self-subsistent entity or thing; existing in its own right; not derivative or dependent. Enduring or permanent, as distinguished from transitory. Belonging to the essence or intrinsic nature of the substance, as distinguished from something that is accidental or qualifying – i.e., essential.

Perhaps oddly, this term – although used in Paragraph 1-12, AR 25-1, in application to information quality – is not defined in documents guiding the QI, such as AR 25-1, DA PAM 25-1-1, or the SECDEF's memo on QI guidelines (see <http://www.defenselink.mil/pubs/guidance2.html>). The preceding definition is from *Webster's Third New International Dictionary* (unabridged). AR 25-1 states that “[o]rganizations will not disseminate substantive information that does not meet a basic level of quality” – in this context, the meaning of *substantive* aligns most closely with Webster's second meaning of *enduring* or *permanent*.

System of records

A group of records under the control of DA from which information is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned to the individual. System notices for all systems of records must be published in the *Federal Register*. (A grouping or files series of records arranged chronologically or subjectively that is not retrieved by individual identifier is not a system-of-records, even though individual information could be retrieved by such an identifier, such as through a paper-by-paper search.) [Section II of glossary, AR 340-21]



Technical control

The authority for one organization or command to issue and enforce policy and authoritative direction concerning the use of techniques, procedures, standards, configurations, designs, devices, and systems to another specified organization to accomplish a specific mission. Technical control does not include command authority or administrative control for logistics or matters of administration, discipline, internal organization, or unit training. [Section II of glossary, AR 25-1]

Template

In the sense of Web development and design, a template is a special type of document used to design a “locked” page layout. A template author designs the page layout and creates regions in the template that are editable in documents that are based on a template. In a template, the designer controls which page elements a template user – such as writers, graphic artists, or other Web developers – can edit.

The “templates” offered in Appendix L serve as models or guides (another meaning of the word “template”) to use for adoption / adaptation regarding required Army content.

Third-party cookies

Cookies placed on a user’s hard drive by Internet advertising networks. The most common third-party cookies are placed by the various companies that serve the banner ads that appear across many Websites. [Section II of glossary, AR 25-1]

Token

A device (e.g., floppy disk, CAC, smart card, PC card, Universal Serial Bus (USB) device, etc.) that is used to protect and transport the private keys of a user. The primary hardware token selected for DoD use is the CAC. [Attachment in memorandum from the ASD-C3I, “Public Key Enabling (PKE) of Applications, Webservers, and Networks for the Department of Defense (DoD)”; attachment in memorandum from ASD-C3I, “Department of Defense (DoD) Public Key Infrastructure (PKI)”]

TRADOC subordinate organization

Also referred to in TRADOC regulations as TRADOC mission activity or command / activity, any organization assigned to TRADOC and assisting in this Army command’s mission / core functions of training (IMT, functional and collective training, and training support), and educating the Army’s Soldiers; developing its leaders; developing doctrine; establishing standards; and building the future Army through concepts development, experimentation and requirements determination. TRADOC also consolidates and applies the Army’s lessons-learned.

TRADOC consists of HQ TRADOC and several MSOs: U.S. Combined Arms Center (USACAC), U.S. Army Combined Arms Support Command (USACASCOM), U.S. Army War College (USAWC), U.S. Army Sergeants Major Academy (USASMA), Army Management Staff College (AMSC), Warrant Officer Career Center (WOCC), TRADOC Analysis Center (TRAC), U.S. Army Aeronautical Services Agency (USAASA), Defense Language Institute Foreign Language Center (DLIFLC), Western Hemisphere Institute for Security Cooperation (WHINSEC), and U.S. Disciplinary Barracks (USDB). Although established as a FOA, ARCIC is an integral part of, and functions as an element of, the HQ TRADOC staff.

(**Note:** As of Oct. 1, 2008, U.S. Army Accessions Command (USAAC) – which includes U.S. Army Recruiting Command (USAREC), U.S. Army Cadet Command (USACC) and U.S. Army Accessions Support Brigade (USAASB) – began to report directly to the SecArmy / CSA, per the SecArmy’s direction. The IMT mission, however, remains with TRADOC. HQ TRADOC has a DCG dedicated to the “IMT enterprise” who reports directly to the TRADOC CG. (The CSA approved the IMT enterprise Sept. 24, 2008.) The DCG-IMT has detailed oversight and command authority of the IMT enterprise, senior-rates training-brigade commanders, centrally manages IMT resourcing, and exercises C2 of the BCT CoE. This plan began its initial operating capability Oct. 1, 2008, and will bridge to full operating capability in the near future.)

USACAC includes Combined Arms Doctrine Directorate (CADD), Combined Arms Center-Training (CAC-T), Command and General Staff College (CGSC), TRADOC Program Integration Office Battle Command (TPIO-BC),

and Center for Army Lessons Learned (CALL). USACASCOM will be the hub of the Sustainment CoE. Both commands will have CoEs aligned under them.

BRAC 2005 decisions and CoE required moves are changing the TRADOC organizational structure between Fiscal Years (FY) 2009 and 2011. TRADOC is moving about one-fifth of its workforce (about 11,000 positions); standing up four multi-branch CoEs, four single-branch CoEs, and three Joint schools; moving five schools and 186 courses; moving an annual student load of more than 32,000 people; overseeing more than \$4 billion in construction; moving USAAC, USACC, and TRADOC HQ – all while supporting an Army at war. Target date for this to be accomplished is Sept. 15, 2011. TRADOC will reorganize from 13 centers / schools to eight CoEs.

Multi-branch CoEs standing up include:

- Fires CoE – combining the Field Artillery School, already at Fort Sill, Okla., and Air Defense Artillery School, Fort Bliss, Texas – at Fort Sill;
- Maneuver CoE – combining the Armor School at Fort Knox, Ky., and Infantry School already at Fort Benning, Ga. – at Fort Benning;
- Maneuver Support CoE – essentially MANSCEN renamed and remaining at Fort Leonard Wood, Mo. (MANSCEN includes the Army's Engineer, Chemical and Military Police schools); and
- Sustainment CoE – combining at Fort Lee, Va., the Ordnance Center (including Ordnance Mechanical Maintenance School (OMMS) from Aberdeen Proving Ground, Md., and Ordnance Mission and Electronic Maintenance School (OMEMS), Redstone Arsenal, Ala.), Soldier Support Institute (Adjutant General and Financial Management schools at Fort Jackson, S.C.), Army Chaplain Center / School, Fort Jackson; Armed Forces School of Music, Army Element, at Fort Eustis, Va.; Army Medical Department Center / School, Fort Sam Houston, Texas; Quartermaster Center / School, Fort Lee; Transportation Center / School, Fort Eustis; Recruiting and Retention School, Fort Jackson; Reserve Mobilization and Training Center, Fort Lee; and Army Logistics Management College, Fort Lee.

Single-branch CoEs standing up include:

- Aviation CoE, converting from the Aviation School, Fort Rucker, Ala.;
- Intelligence CoE, formerly the Intelligence School, Fort Huachuca, Ariz.;
- Signal CoE, comprising the Signal School, Fort Gordon, Ga.; and
- BCT CoE, made from the U.S. Army Training Center at Fort Jackson, S.C. (formerly aligned under USAAC).

USAAC and its subordinate commands USACC and USAREC, plus the Human Resource Command, are combining into the Human Resource CoE, a direct reporting unit (DRU) to the SecArmy, at Fort Knox, Ky. The stand-up of the three Joint schools will relocate the Joint Transportation Management and Joint Culinary Schools from Lackland Air Force Base (AFB), Texas, to Fort Lee. The Armed Forces Chaplaincy Center, scattered from Maxwell AFB, Ala.; Naval Air Station Meridian, Miss.; and Naval Station Newport, R.I.; will consolidate at Fort Jackson.

See TR 10-5.

TRADOC Website

Any Website where the content is developed / maintained by or at the request of a TRADOC activity or subordinate organization. [definition by TRADOC Webmaster, G-6, via email Nov. 20, 2006]

Transparent / transparency

The practice of describing the data and methods of developing an information product in a way that it would be possible for an independent individual or organization to reproduce the results. [Paragraph 11, Attachment 2, memorandum from the DEPSECDEF, "Ensuring Quality of Information Disseminated to the Public by the Department of Defense"]

Twitter

A micro-blogging site. (Micro-blogging features posts and links in 140 characters or less.) Many people link Twitter to their cellphones to update on the go. Since long URLs are difficult to fit in 140 characters, URL-shortening sites like bit.ly and tiny.url compress URLs to under 15 characters for copying and pasting into a *tweet*.

(A message on Twitter is called a “tweet.”) The Army is currently using [bit.ly](#) because it allows users to track how many clicks a link has received.



Unclassified protected information

Information that includes the categories of CUI, sensitive, FOUO, critical, OPSEC indicators, and PII. These categories are not classified but still must be protected against dissemination on a publicly accessible Website.

Uniform Resource Locator

The Internet addressing scheme that defines the route to an Internet resource – such as a document, file, Webpage, or application on the Internet – via a browser program. More simply, a fairly user-friendly “Web address” that a person uses to direct his / her browser to a particular Internet resource – all Web addresses have a URL. The URL contains four distinct parts: protocol type, machine name, directory path, and file name. For example: <http://www.tradoc.army.mil/pao/index.html>, where *http* is the protocol; *www.tradoc.army.mil* is the TLD name as well as the machine name; *pao* is the directory path; and *index.html* is the file name. [Section II of glossary, AR 25-1; Section II of glossary, DA PAM 25-1-1]

Unofficial Website

A DoD Website that is developed and maintained with non-appropriated funds, and for which the DoD component, or a subordinate organization, does not usually exercise editorial control over content. The content of unofficial DoD Websites is not endorsed as the official position of the DoD component. Content will not normally include official news releases, installation history, command position papers, etc. Unofficial DoD Websites may include sponsorships and commercial advertisements, and may also advertise products for sale, IAW the organization’s mission. In most cases, unofficial DoD Websites are developed and maintained by commercial or nonprofit organizations. Certain military-affiliated organizations may develop and maintain unofficial DoD Websites. Such organizations include service exchanges and morale, welfare, and recreation activities that use non-appropriated funds. [Part III, DoD Website policy]

Website created on personal time, not produced in connection with military duties, and not funded with DoD funds. [Paragraph 13-14d, AR 360-1]

User ID

Unique symbol or character string that is used by an IS to uniquely identify a specific user. [Section II of glossary, AR 25-2]

Utility

Standard of the QI Program. Refers to the relevance and timeliness of information to its intended users, including the public. In assessing the usefulness of information that the component disseminates to the public, the component needs to consider the uses of the information not only from the perspective of the component but also from the perspective of the public. [Paragraph 12, Attachment 2, memorandum from the DEPSECDEF, “Ensuring Quality of Information Disseminated to the Public by the Department of Defense”]



Video

Motion imagery that is recorded or transmitted as either a digital or analog electromagnetic signal. [Enclosure 1, memorandum from the ASD-PA, “Visual Information (VI) Activity Management”]

Video-sharing

Allows individuals to produce their own unique video content and host it on the Web. With the rise in mobile video (uploading video from a cellphone) and the accessibility of video-recording devices, video-sharing is on the rise. There are dozens of sites offering free hosting of user-uploaded video content. YouTube and Vimeo, <http://www.youtube.com> and <http://www.vimeo.com/>, are two of the largest sites. YouTube currently dominates the video-sharing market and has the most name recognition of any site of its kind; however, because YouTube is such a

large and diverse community, it is inundated with garbage video and immature users. Vimeo represents a smaller portion of the video-sharing market. Videos posted to Vimeo should be polished and can be uploaded as high-resolution video, as Vimeo's users are accustomed to thought-provoking and artistic content.

Vision

A description of the future; the most abstract description of the desired end-state of an organization or activity at an unspecified point in the future. [Section II of glossary, AR 25-1]

An organization's view of how it would like to be perceived by its customers at some future point. It is the organization's ideal, providing a focus for efforts and goal-setting. [Section II of glossary, AR 5-1]

Visual information

Information in the form of visual or pictorial representation of person(s), place(s), or thing(s), either with or without sound. VI includes still photographs, digital still images, motion pictures, analog and digital video recordings, graphic arts, visual aids, models, displays, visual presentation services, and the processes that support them; it includes hand- or computer-generated art and animations that depict real or imaginary person(s), place(s), and / or thing(s), and related captions, overlays, and intellectual control data. VI is the element of IT that addresses the acquisition, creation, storage, transmission, distribution, and disposition of still and motion imagery and multimedia, with or without sound, linear or nonlinear, for the purpose of conveying information. VI includes the exchange of ideas, data, and information regardless of formats and technologies used (see DoDD 5040.3). The VI mission is to provide Army commanders with combat camera (COMCAM) and record documentation, multimedia/VI products, and services to satisfy official requirements. These requirements may include, but are not limited to, support for C2, training, education, logistics, medical, personnel, special operations, engineers, public affairs, and intelligence to effectively convey accurate information to the warfighter, decision-makers, and supporting organizations. [Glossary, DoDI 5400.13; Enclosure 1, memorandum from the ASD-PA, "Visual Information (VI) Activity Management,"; Paragraph 7-1 and Section II of glossary, AR 25-1; Section II of glossary, DA PAM 25-1-1]

Visual-information documentation program

VI documentation (VIDOC) provides a visual record of significant Army events and activities. This information is acquired for operational, training, and historical purposes. The VIDOC program includes both tactical and non-tactical documentation. We are concerned here with non-tactical documentation, such as that which PAOs use to keep Army personnel informed and for release to the news media. Non-tactical (infrastructure) documentation is record documentation of technical, operational, and historical events as they occur during peacetime. This documentation provides information about people, places, and things as well as processes in the fields of medicine, science, logistics, RDT&E, and other historical events. Non-tactical record documentation includes linear and digital video, photographic imagery, graphic artwork (including recruiting and safety posters/artwork), or audiotape. [Paragraphs 7-10 and 7-10b(1) and (4), AR 25-1]

Vlog

On-line video blog that can be downloaded to devices such as PCs or handheld devices (wireless phones, mp3 players, iPods). These can be subscription-based or free, single-use, or repeated-use content. Also called a video-based diary, it is a Webpage maintained as a journal for personal comments and video images. It may include hyperlinks to other Webpages. [Paragraph 13-14d, AR 360-1]



Warning banner

Verbiage that a user sees or is referred to at the point of access to a system which sets the right expectations for users regarding acceptable use of a computer system and its resources, data, and network-access capabilities. These expectations include notice of authorized monitoring of users' activities while they are using the system, and warnings of legal sanctions should the authorized monitoring reveal evidence of illegal activities or a violation of security policy. [Section II of glossary, AR 25-2]

Web log (blog)

A blog (an abridgment of the term *web log*) is a frequently updated, conversational Website, typically offering news or opinion on a specific topic. Blogs are chronologically ordered, commonly displaying entries in reverse chronological order. A blog also usually includes permanent hyperlinks to other sources, creating a historical archive. “Blog” can also be used as a verb, meaning to maintain or add content to a blog. Many blogs provide commentary or news on a particular subject; others function as more personal on-line diaries. A typical blog combines text, images, and links to other blogs, Webpages, and other media related to its topic. The ability for readers to leave comments in an interactive format is an important part of many blogs. Most blogs are primarily textual – although some focus on art (artlog), photographs (photoblog), sketchblog, videos (vlog), music (MP3 blog) or audio (podcasting) – and are part of the wider network of social media. [Paragraph 13-14d, AR 360-1; <http://en.wikipedia.org/wiki/BLOG>]

Web content

Information on a Webpage or Web application, or information which is sent from a server to a browser via HTTP, HTTPS, or FTP when a URL has been activated. Content on a Webpage therefore includes not only text but also buttons and other visual navigational aids, images, forms, hyperlinks, sounds, and other hypermedia, or other elements. [<http://www.w3.org/WAI/intro/wcag.php>, accessed Sept. 21, 2006]

For purposes of Army Web-content records to be transferred to NARA, Web content is limited to what is accessed over HTTP from a server to a client browser when a URL has been activated. (All other transfer protocols (i.e., FTP and SMTP) are excluded.) Web content for NARA includes records that share a domain name, including content managed under formal agreement and residing on another site (such as a civilian contractor’s site); all component parts of Web-content records that have been appraised as permanent, including image, audio, video, and all other proprietary formats; and static and dynamic content. (Web content is rendered in two forms: static and dynamic. Static Web content consists of information in the form of “Web documents” that are rendered identically each time they are accessed. Dynamic Web content consists of information that is rendered differently based on specific user input and is usually managed in a database associated with a server.) [<http://www.archives.gov/records-mgmt/initiatives/web-content-records.html>, accessed June 9, 2006]

Webpage or page

The term *page* is used to represent every Webpage or file related to, and linked from, any files that contain DoD information on a unit or activity’s Internet site, regardless if it is on an unclassified or a classified local-area network (LAN). This includes embedded items, such as graphics, multimedia, etc. [Paragraph E-5, AR 380-5]

An individual HTML-compliant electronic file accessible through a TCP / IP network. [Section II of glossary, AR 380-5. Also, memorandum from DISC4, “Guidance for Management of Publicly Accessible U.S. Army Websites”]

Web portal

Website serving as a starting point to other destinations or activities on the Web. Initially thought of as a “home base” type of Webpage, portals attempt to provide all a user’s Internet needs in one location. Portals commonly provide services such as email, collaboration centers, on-line chat forums, searching, content, newsfeeds, and others. [Section II of glossary, AR 25-1]

Webserver

A Website including hardware and software that includes the operating system, Web software, other software and data, or the software that manages Web functions at a Website. [Section II of glossary, DA PAM 25-1-1]

Website

A location on the Internet; specifically it refers to the point-of-presence (POP) location in which it resides. All Websites are referenced using a special addressing scheme called a URL. A Website can mean a single HTML file or hundreds of files placed on the net by an enterprise. [Section II of glossary, AR 25-1]

A computer on the Internet or an intranet running a Webserver that responds to HTTP and HTTPS requests from Web browsers. [Section II of glossary, DA PAM 25-1-1]

A collection of information in HTML-compliant electronic files, organized and relating to a common subject or set of subjects, and designed to provide information, services, or goods to users through a TCP / IP network. Includes the homepage and linked subordinate information. [Part III, DoD Web policy; Section II of glossary, AR 380-5]

A Website includes a “homepage” and the linked subordinate information. [TR 25-1]

A related collection of Web content identified by a domain name. [Glossary, <http://www.archives.gov/records-mgmt/initiatives/web-content-records.html>, accessed June 9, 2006]

Wiki

Collaborative publishing technology that allows multiple users to work on and publish documents on-line with appropriate version control. Wikis allow hypertext links to content in any form, enhancing user experience and interactions.

Worldwide Web

The subset of the Internet capable of providing the public with user-friendly, graphics-based, multimedia access to information on the Internet. It is the most popular means for storing and linking Internet-based information in all multimedia formats. Navigation is accomplished through a set of linked documents that may reside on the same computer or on computers located almost anywhere else in the world. [Part III, DoD Website policy]

A part of the Internet designed to allow easier navigation of the network through the use of graphical user interfaces (GUI) and hypertext links between different addresses – called also *Web*. A function for sharing documents with text and graphic content that links documents locally and remotely. [Section II of glossary, AR 25-1; Section II of glossary, DA PAM 25-1-1]

The universe of accessible information available on many computers spread through the world and attached to that gigantic computer network called the Internet. The Web encompasses a body of software, a set of protocols, and a set of defined conventions for accessing the information on the Web. The Web uses hypertext and multimedia techniques to make the Web easy for anyone to roam, browse, and contribute to. The Web makes publishing information (that is, making that information public) as easy as creating a *homepage* and posting it on a server somewhere in the Internet. Also called *W3*. [Section II of glossary, AR 25-2]



YouTube

An on-line site for uploading and discussing videos; videos can also be embedded from YouTube onto other social-media sites such as blogs or social networks.

Appendix C

Key management control checklist

AR 25-1 mandates the key management control checklist in its Appendix C as a required checklist; the following reproduces that checklist as applicable to Web content. The checklist poses questions for content reviewers to check for prohibited and required information. Answers to those questions must be based on actually testing management controls, such as via document analysis, direct observation, sampling, and simulation. Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation.

These key management controls must be formally evaluated at least once every five years.

The numbering of the test questions that follow parallels that of Paragraph C-4e, AR 25-1, for easier cross-reference:

- (25) Are existing portals being migrated to AKO / DKO and AKO-S?
- (26) Does each Website contain a clearly defined purpose statement that supports the mission of the organization?
- (27) Are users of each publicly accessible Website provided with a privacy and security notice prominently displayed or announced on at least the first page of all major sections of each Web information service (WIS)?
- (28) If applicable, does the Website contain a disclaimer for an external-links notice for any site outside of the official DoD WIS (usually the .mil domain)?
- (29) Is this Website free of commercial sponsorship and advertising?
- (30) Is the Website free of persistent cookies or other devices designed to collect PII about Web visitors?
- (31) Is each Website made accessible to handicapped users in accordance with Section 508 of the Rehabilitation Act?
- (32) Is operational information identified below purged from publicly accessible Websites?
 - (a) Plans or lessons learned that would reveal military operations, exercises, or vulnerabilities.
 - (b) Sensitive movements of military assets or the location of units, installations, or personnel where uncertainty regarding location is an element of the security of a military plan or program.
 - (c) Personal information about U.S. citizens, DoD employees, and military personnel, to include the following:
 - Social Security account numbers
 - Dates of birth
 - Home addresses
 - Directories containing name, duty assignment, and home telephone numbers
 - Names, locations, or any other identifying information about family members of DoD employees or military personnel
 - (d) Technological data such as:
 - Weapon schematics
 - Weapon-system vulnerabilities
 - Electronic wire diagrams
 - Frequency-spectrum data
- (33) Are OPSEC tip-off indicators in the following categories purged from the organization's publicly accessible Website?
 - (a) Administrative
 - Personnel travel (personal and official business)
 - Attendance at planning conferences
 - Commercial support contracts
 - FOUO
 - (b) Operations, plans, and training
 - Operational orders (OPORDs) and plans (OPLANs)
 - Mission-specific training
 - Exercise and simulations activity
 - Exercise, deployment, or training schedules
 - Unit relocation / deployment
 - Inspection results, findings, deficiencies
 - Unit vulnerabilities or weaknesses
 - (c) Communications
 - Spectrum emissions and associated documentation

- Changes in activity or communications patterns
- Use of Internet and / or email by unit personnel (personal or official business)
- Availability of secure communications
- Hypertext links with other agencies or units
- Family-support plans
- Bulletin board / messages between Soldiers and family members
- (d) Logistics / maintenance
 - Supply and equipment orders / deliveries
 - Transportation plans
 - Mapping, imagery, and special documentation support
 - Maintenance and logistics requirements
 - Receipt or installation of special equipment
- (34) Has the Website reviewer performed a keyword search for any of the following documents and subsequently removed sensitive personal or unit information from publicly accessible Websites?
 - Deployment schedules
 - Duty rosters
 - Exercise plans
 - Contingency plans
 - Training schedules
 - Inspection results, findings, deficiencies
 - Biographies
 - Family-support activities
 - Phone directories
 - Lists of personnel

The numbering of the test questions that follow parallels that of Paragraph C-4g, AR 25-1, for easier cross-reference:

- (1) Is a records-management program established in your organization?
- (2) Has a records official been appointed to manage the internal records of the organization and its sub-elements?
(See Chapter 5 of this **Guide**; Webpages / Websites may be determined as official Army records.)
- (7) Do all information collections [on the Website] from the public, affecting 10 or more individuals, have OMB approval?

Appendix D

Required notices

Verbiage for the privacy and security, cookie, and other required notices, such as the external-links disclaimer and the access-control notice, are outlined, following.

DOD STANDARD PRIVACY AND SECURITY NOTICE

The DoD Web policy (Paragraph 4, Part V) provides the following text for an organization's required privacy and security notice that may be tailored by each organization sponsoring a publicly accessible Website. The notice must be approved by local legal authority before use. The link to the following text must be labeled "Privacy policy" and must at least be on the homepage. Key: () indicates sections to be tailored at the installation level. [] indicates hyperlinks. * indicates information located at the hyperlink destination indicated.

1. (Name of Website) is provided as a public service by the [sponsor].
2. Information presented on (name of Website) is considered public information and may be distributed or copied. Use of appropriate byline / photo / image credits is requested.
3. For site management, [information is collected]* for statistical purposes. This government computer system uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.
4. For site security purposes and to ensure this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.
5. Except for authorized law-enforcement investigations, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with [National Archives and Records Administration (NARA) guidelines].
6. Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1987 and the National Information Infrastructure Protection Act.
7. If you have any questions or comments about the information presented here, please forward them to (us using the Website name) [comment form or other means of contact].

*Link from [information is collected] above to the following text (*note*: the following information should be tailored, if necessary to show an accurate example of the specific information being collected):

Example: information collected from (name of Website) for statistical purposes

Below is an example of the information collected based on a standard request for a Worldwide Web document:

xxx.yyy.com – [28/Jan/1997:00:00:01 -0500] "GET /DefenseLINK/news/nr012797.html HTTP/1.0" 200 16704 Mozilla 3.0/www.altavista.digital.com

xxx.yyy.com (or 123.123.23.12) – This is the host name (or IP address) associated with the requester (you as the visitor). In this case, the requestor (xxx.yyy.com) is coming from a commercial address. Depending on the requester's method of network connection, the host name (or IP address) may or may not identify a specific computer. Connections via many Internet service providers assign different IP addresses for each session, so the host name identifies only the ISP. The host name (or IP address) will identify a specific computer if that computer has a fixed IP address.

[28/Jan/1997:00:00:01 -0500] – This is the date and time of the request.

"GET /DefenseLINK/news/nr012797.html HTTP/1.0" – This is the location of the requested file on (DefenseLINK).

200 – This is the status code – 200 is OK – the request was filled.

16704 – This is the size of the requested file in bytes.

Mozilla 3.0 – This identifies the type of browser software used to access the page, which indicates what design parameters to use in constructing the pages.

www.altavista.digital.com – This indicates the last site the person visited, which indicates how people find (name of Website).

Requests for other types of documents use similar information. No personally-identifying information is collected.

Agencies subject to DoDD 5240.1 (DoD intelligence activities) shall add the following to Paragraph 5: All data-collection activities are in strict accordance with DoD Directive 5240.1.

DOD STANDARD COOKIE DISCLAIMER

The DoD Web policy (Paragraph 4, Part V) provides the following text, which may be used as a notice for organizational sites using session cookies. Tailor where text appears in parentheses:

(Name of Website) does not use persistent cookies – i.e., tokens that pass information back and forth from your machine to the server and remain after you close your browser. (Name of Website) does use session cookies – i.e., tokens that remain active only until you close your browser – to make the site easier for you to use. No database of information obtained from these cookies is kept, and when you close your browser, the cookie is deleted from your computer. (Name of Website) uses cookies in the following ways:

- (Describe use, e.g., “to save you time in filling out forms,” “to maintain a relationship between the image and the correct link, the program that displays the banners on the bottom of some of our pages uses a session cookie.”)

You can choose not to accept these cookies and still use the site, but (you may need to enter the same information repeatedly and clicking on the banners will not take you to the correct page). The help information in your browser software should provide you with instruction on how to disable cookies.

DOD STANDARD EXTERNAL-LINKS DISCLAIMER

DoD Web policy (Paragraph 7.2, Part II) and Army policy and guidance (Paragraph 6-7c, AR 25-1) require that each Website have a page (posted or linked to) that explains the organization’s process for linking to non-government Websites and includes its guidelines for selecting and maintaining external links. The process, and therefore the on-line explanation, must consider Army policy, which states: “Army commands and activities will establish objective and supportable criteria or guidelines for the selection and maintenance of links to external Websites. Guidelines should consider the information needs of mission-related requirements and public-communications and community-relations objectives. ... Listings of Web links on Army Webpages must separate external Web links from government and military links.”⁶⁰⁴ Further, the link “must exhibit sound public policy and support the Army’s mission. Organizations’ linking procedures must explain why some links are chosen and others are not. Links must be chosen fairly and in the best interest of the public.” This link-explanation content should be included in the organization’s “Important Notices” page.

Additionally, organizations must comply with DoD’s / DA’s requirement that when external links to non-government Websites are included, the following disclaimer must appear on each page listing external links or through an intermediate “exit notice” page activated by the server when the external link is clicked (whenever a server request is made for any Website other than the official DoD Website, which is usually on the dot-mil domain):

The appearance of external hyperlinks does not constitute endorsement by the U.S. Army of this Website or the information, products or services contained therein. For other than authorized activities such as military exchanges and MWR sites, the U.S. Army does not exercise any editorial control over the information you may find at these locations. Such links are provided consistent with the stated purpose of this Website.

An example of an exit notice is located on the White House’s site, <http://www.whitehouse.gov/>.

⁶⁰⁴ Paragraph 6-7c(7), AR 25-1.

DOD STANDARD ACCESS-CONTROL NOTICE AND CONSENT BANNER

DoD Web policy (Paragraph 3.6.3, Part II) is that sites with access controls are not linked from publicly accessible Websites except in some circumstances: “Publicly accessible DoD Websites will not normally contain links or references to DoD Websites with security and access controls. Under certain circumstances, however, it may be appropriate to establish a link to a log-on site provided details as to the controlled site’s contents are not revealed.”

When an access-controlled site (requires log-on) is linked from the publicly accessible Web, DoD Web policy (Paragraph 4.2, Part V) requires a specific notice and consent banner. (The best way to handle this is to provide the banner as a pop-up exit notice when the Website visitor clicks on the link to the access-controlled site, or as landing page once the visitor follows the link – either way, the visitor must take action to read and accept the terms stated in the banner.) The banner is approved by the DoD CIO; deviations are not permitted except as authorized in writing by the Deputy Assistant SECDEF for Information and Identity Assurance:

You are accessing a U.S. government (USG) information system (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests – not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

DOD PA / PAS STATEMENTS

DoD Web policy allows that, in certain instances, it’s necessary and appropriate to collect information from Website visitors – such as during the yearly Website-user assessment – but agencies that do so (see privacy and security notice section, above) must comply with the following provisions as well (see Paragraph 11, Part II, DoD Web policy).

Compliance with the PRA. Publicly accessible Websites must comply with the requirements of the PRA of 1995. The PRA requires that collection of information from the public be approved by OMB under some circumstances:

- Requests for identical information from 10 or more members of the public, to include DoD contractors, must be approved by OMB. Such requests include surveys using checkbox, radio button, or text form fields.
- The PRA applies to electronic forms / information collections on Websites that **collect standardized information** from the public. It does not apply to collection of information strictly from current DoD employees or service members in the scope of their employment. Surveys on publicly accessible Websites will not ordinarily be exempt from the requirement to obtain OMB approval under this exception.
- Forms for general solicitations of comments that do not seek responses to standard questions, such as the common opinion-based feedback forms and email links, do not require OMB clearance. See, however, below on use of a PA.

The PRA requires a feedback mechanism for users’ comments, which dovetails with the organization’s requirement to collect information as part of its yearly assessment. Organizations are responsible for ensuring their publicly accessible Websites comply with this requirement and follow procedures in DoD 8910.1-M, *Department of Defense Procedures for Management of Information Requirements*, <http://www.dtic.mil/whs/directives/corres/pdf/891001m.pdf>. (Especially see Paragraph C2.2 and Chapter 3.) The

method of collection⁶⁰⁵ – i.e., the Internet – does not affect the requirement, only whether identical questions are asked of 10 or more persons.⁶⁰⁶

Collection of user-identifying information from DoD Websites. The solicitation or collection of PII, including collection through capabilities which allow a user to contact the Website owner or Webmaster, triggers the requirement for either a PA or a PAS.

Use of a PAS – The Army privacy regulation (Paragraph 4-2, AR 340-21) requires that whenever PII is requested from an individual that will become part of a *system of records* – retrieved by reference to the individual’s name or other personal identifier – the individual will be furnished a PAS. This statement is to ensure that individuals know why their PII is being collected so they can make an informed decision on whether or not to furnish it. As a minimum, the PAS must include the following information in language that is explicit and easily understood, and not so lengthy as to deter an individual from reading it:

- Cite the specific statute or executive order, including a brief title or subject, which authorizes the Army to collect the PII requested. Inform the individual whether or not a response is mandatory or voluntary, and any possible consequences of failing to respond.
- Cite the principal purposes for which the information will be used.
- Cite the routine uses for which the information may be used. This may be a summary of information published in the applicable system notice.

Applicable to the Web, whenever PII is solicited from an individual and, again, the information is maintained in a Privacy Act *system of records* (see Chapter 3), a PAS must be posted to the Webpage where the information is being solicited or provided through a well-marked hyperlink. If the information collected is being maintained in a Privacy Act system of records for which a notice has not yet been published in the *Federal Register*, such a notice must be published, consistent with the requirements of the Privacy Act, prior to any information being collected. If a PAS would be required if the solicitation were made in the paper-based world, it is required in the on-line world, whether the site is publicly accessible or non-publicly accessible.⁶⁰⁷

Thus we highly recommend that user assessments use open-ended questions that enable the user to respond anonymously and avoid collecting any PII if possible. (Even providing an email address is collecting PII, as the email address contains the name of the individual).

Use of a PA – If PII is solicited by a DoD Website (for instance, collected as part of an email feedback / comments feature on a Website) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a PA. The PA informs the individual as to why the information is being solicited (so that the organization can provide the information that has been requested by the individual, for example) and how such information will be used (for example, it will be destroyed after the information the individual is seeking has been forwarded to him or her). If PII is solicited by a DoD Website (e.g., as part of electronic commerce transactions), a PA must be provided regardless of where the information is maintained. The PA must be posted to the Webpage where the information is being solicited or provided through a well-marked hyperlink. Providing a statement such as “Privacy advisory: please refer to the privacy and security notice that describes why this information is being collected and how it will be used,” linked to the applicable portion of the privacy and security notice required above, is satisfactory.⁶⁰⁸

Automated collection of information on publicly accessible Websites. Collecting information will employ use of cookies. As stated, use of *session cookies* is permitted for session control and to maintain state, but these cookies must expire at the end of the logical session. Data from those cookies may not be used for other purposes or stored.

⁶⁰⁵ IAW Paragraph C3.6.9.1, DoD 8910.1-M, an electronic questionnaire attached to an Internet site, which asks identical, specific questions of 10 or more people, is subject to OMB review and approval. The approved electronic format must display the OMB approval number and expiration date.

⁶⁰⁶ Refer to Paragraph C3.6.9.2, DoD 8910.1-M, which states: “An Internet ‘suggestion box’ format such as one requesting ‘ideas, comments, suggestions, or anything else you would like to tell us,’ or one asking ‘if you experience any technical problems with our site, or have any suggestions for improving it, please let us know,’ are not considered to be identical questions. Such general solicitations of comments from the public do not require OMB approval.” See Paragraph C3.8.2 in the manual for details on the exemptions to the OMB-approval policy.

⁶⁰⁷ See Paragraph 11.2.1, Part II, DoD Web policy.

⁶⁰⁸ See Paragraph 11.2.2, Part II, DoD Web policy.

The use of session cookies must be explicitly identified in the site's privacy notice. (See Paragraph 4.1, Part V, DoD Web policy, and "privacy and security notice" section above.)

Use of persistent cookies is authorized **only** if **all** of the following conditions are met:

- There is a compelling need to gather the data on the Website;
- Appropriate technical procedures have been established to safeguard the data;
- The SECDEF has personally approved use of the cookie prior to implementation of the data collection; and
- Privacy notices clearly specify, in addition to other required information, that cookies are being used and describe the safeguards for handling the information collected from the cookies.

Requests for approval to use persistent cookies should be submitted at least 30 days prior to the operational-need date, through the appropriate chain of command, to the office of the ASD-NII / DoD CIO for processing prior to submission to the SECDEF for decision. The request shall describe the need and the safeguards to be used to protect the data, provide an explanation of why other technical approaches are inadequate, and include a copy of the privacy notice(s) proposed for use.⁶⁰⁹

Other automated means of collecting information. Except for system log files / site-usage data addressed in the next paragraph, using any other automated means to collect information requires the same approvals as described in the above paragraph.

Usage statistics. As a management function, evaluation of site-usage data (log files) is a valuable way to evaluate a Website's effectiveness. However, per DoD policy, collection of data from publicly accessible sites for undisclosed purposes is inappropriate. There are commercially available software packages that will summarize log-file data into usable statistics for management purposes, such as the most / least requested documents, type of browser software used to access the Website, etc. Use of this type of software is appropriate as long as there is full disclosure as specified in the privacy and security notice. Organizations must establish a destruction disposition schedule for collected data.

DOD PLATFORM FOR PRIVACY PREFERENCES PROJECT NOTICE

According to the DoD Web policy (Paragraph 6, Part II), a Website's privacy policy and Platform for Privacy Preferences Project (P3P) notice must meet these standards:

- IAW the privacy provisions of the E-Government Act of 2002, all publicly accessible Websites must have both a "human readable" privacy policy and machine-readable technology that automatically alerts users about whether site privacy practices match their personal privacy preferences.
- The human-readable privacy policy, as stated in the "privacy and security notice" section above, must describe how, in general, security is maintained on the site, what specific information is collected, why it is collected, and how it is used. All information collected must be described in this policy.
- The link to the human-readable version must be labeled "privacy policy," as stated, and must be prominently displayed on the homepage and major entry points to the Website.
- According to the W3C, the P3P enables Websites to "express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents. P3P user agents will allow users to be informed of site practices (in both machine- and human-readable formats) and to automate decision-making based on these practices when appropriate. Thus users need not read the privacy policies at every site they visit." The DoD Web policy (Paragraph 6, Part II) states that P3P (<http://www.w3.org/P3P/>) is the standard for machine-readable privacy policy; each Website must include not only a human-readable policy but a machine-readable policy IAW the P3P's recommendations. An example of a DoD machine-readable privacy policy in use is Defense Information System Agency's (DISA) at <http://www.disa.mil/w3c/p3p.xml>.

Organizations will avoid flashy graphics or other indicators that create a misperception of danger, such as skull-and-crossbones logos or "warning" signs, associated with their privacy notice or any other notice / banner.

Training resources and best-practice guidance are available at Webcontent.gov, "Your Guide to Managing U.S. Government Websites."

⁶⁰⁹ See Paragraph 11.3, Part II, DoD Web policy.

Appendix E

Examples of critical information

- Courses of action
 - Specific courses of action (COAs) that U.S. and allied commands are planning
 - Specific COAs that U.S. and allied forces cannot undertake or execute
- Forces
 - U.S. and allied forces earmarked for possible COAs
 - Readiness levels of organizations
 - Specific current force / unit locations
 - Specific projected force / unit locations
- Command and control
 - U.S. and allied command arrangements for executing COAs
 - Current or future locations of unit commanders
 - Current or future command-post locations
 - Command-post vulnerabilities
- Communications
 - Command, control, communications and computers (C4) and C4 and intelligence (C4I) capabilities
 - Communications site locations
 - Communications limitations (weather, terrain, and equipment shortages, for example)
- Logistics
 - Logistical posture of U.S. and allied forces
 - Speed of deployment / redeployment of ground and air forces
 - Pertinent ground, air, and sea lines of communication (LOCs); locations of storage depots, ports, and airfields
 - Vulnerabilities to interdiction of the LOCs
 - Contents of Army Prepositioned Stocks (APS) and significant restructuring of APS
- Supplies
 - Levels of supplies available for immediate support
 - Pre-positioned supply sites
 - Period of combat sustainment with those supplies
 - Critical item shortages (in all classes)
 - Limitations to resupply capability
 - Demand level for Class IX items
- Locations
 - Specific locations of exercises and operations
 - Specific locations of participating forces
 - Specific projected force / unit locations
 - Alternate force / unit locations
- Vulnerabilities
 - Vulnerabilities of defensive dispositions
 - Vulnerabilities of sensors and other capabilities to detect attack
 - Vulnerabilities to attack
 - Vulnerabilities of units and weapons and weapons systems

- Vulnerabilities in protection or security forces or security plans
- Intelligence
 - Intelligence, surveillance, and reconnaissance (ISR) resources available to support the commander
 - Locations of those ISR capabilities
 - Ongoing ISR operations and their goals
 - Vulnerabilities to exploitation or destruction of those friendly ISR capabilities
- Rules of engagement
 - Policies and rules of engagement (ROE) that govern the use of weapons and electronic or acoustic warfare systems
- Allies
 - Nations providing current or future support to the United States
 - Vulnerabilities that could be exploited to reduce or eliminate such support
- Maintenance
 - Maintenance and salvage capabilities of U.S. and allied forces
 - To what degree these capabilities can support and sustain forces in combat
 - Vulnerabilities to attack
- Weapons
 - Specific characteristics and capabilities of weapons and electronic systems available to coalition forces
 - Doctrine for using various weapons
 - Indicators that unconventional weapons will be employed
 - New weapons that are available or are being employed
 - Vulnerabilities and limitations in friendly weapons and weapons systems
- Psychological operations
 - Intended psychological warfare and subversion operations
 - Plans to exploit adversary vulnerabilities
 - Ongoing operations
 - U.S. agencies conducting operations
 - Psychological operations (PSYOP) themes and objectives
- PSYOP vulnerabilities
 - Vulnerabilities of U.S. forces to psychological warfare and subversion
- Special Operations Forces (SOF) and unconventional warfare
 - Intended sabotage and direct action mission targets
 - Adversary vulnerabilities planned for exploitation
 - Friendly capabilities to conduct unconventional-warfare operations
 - U.S. agencies controlling those resources
 - The SOF team deployment dates
 - The SOF team deployment sites
 - Number of SOF teams / personnel in an area
 - Indigenous support to SOF teams
 - Conventional units associated with SOF teams/personnel
- Deception
 - Planned political and military deceptions
 - Ongoing deception operations

- U.S. agencies conducting deception operations
 - Identity of military units / organizations conducting or participating in deception activities
- Deception vulnerabilities
 - Vulnerabilities of U.S. commanders and staffs to deception
- Counterintelligence
 - U.S. counterintelligence capabilities to detect and neutralize espionage and sabotage nets
 - Number of counterintelligence assets available
 - Identification and location of counterintelligence elements and activities
 - Identification of local personnel that may be assisting friendly counterintelligence forces
- RDT&E programs
 - Weapons systems development schedules (dates, times, locations)
 - Emerging technologies applicable to new weapons systems
 - Computer software used in weapons systems development, testing and evaluation
 - Location of unclassified computer databases used by the RDT&E community
 - Specific contract criteria stated in a classified contract
 - Identification of special access elements within a contract or program
 - Specific Program Protection Plan (PPP) implementation methods
- Medical
 - Casualty figures, both actual and projected
 - VIPs being treated by our medical treatment facilities
 - Overall bed / treatment capacity
 - Increased medical supplies (vaccines, blood products, and so forth) required by unit or theater
 - Shortages in medical MOSs and personnel
 - Identification of projected medical personnel / team deployments
 - Specific identification of classified medical related research programs
 - Identified medical vulnerabilities of friendly forces
- Systems acquisition
 - Corporations or companies projected to be involved in system acquisition
 - Funding amounts of the acquisition program
 - Specifics or requirements of the program in acquisition
 - Classification levels of the program
 - Duration of the acquisition
 - Shortfalls in ability to conduct an acquisition on time to meet requirement
- Government contractors
 - Programs in which the contractor provides classified services and support to the U.S. government
 - Pre-contract award identification of locations of contractor duty
 - Contractor increasing hiring for new or existing contracts or programs
 - Contractor information or service sharing agreements with other private organizations
- Arms control treaty inspections
 - Missions of the activities on the installations to be visited
 - If the installation to be visited is self-sufficient or reliant on the local community for support (that is, telephone service, electricity, water, fire department, police, etc.)
 - If all the buildings on the installation are in use
 - Access to the post

- Morale of installation personnel
 - Condition of the installation
 - Portions of the installation that appear to have more protection / security than other parts of the installation
 - Security procedures in place at this installation (Federal Bureau of Investigation (FBI) support, physical security, counterintelligence activities, law enforcement)
- Information systems
 - IS protection being implemented (measures/procedures)
 - IS approvals / certifications
 - Type of IS equipment protection within an office environment and/or remote site
 - Specific identified vulnerabilities in IS protections at specific locations
- Special Access Programs (SAPs)
 - Organizations and contractors involved in the SAP
 - Mission or subject of the SAP
 - Operational life of the SAP/current stage of development
 - Security procedures for the SAP
 - Budget for the SAP
 - Number of personnel in the SAP
 - Existence and identification of an unacknowledged SAP

For more information, see AR 530-1.

- Diplomatic negotiations
 - Military capabilities (pre-treaty and post-treaty)
 - Intelligence verification capabilities
 - Minimum negotiating positions
- Politico-military crisis management
 - Target selection
 - Timing considerations
 - Logistic capabilities and limitations
 - Alert posture
- Military intervention
 - Intentions
 - Military capabilities
 - Forces assigned and in reserve
 - Targets
 - Timing
 - Logistic capabilities and constraints
 - Limitations
 - Third-nation support arrangements
- Counterterrorism
 - Forces
 - Targets
 - Timing
 - Staging locations
 - Tactics

- Ingress and egress methods
 - Logistic capabilities and constraints
- Open hostilities
 - Force composition and disposition
 - Attrition and reinforcement
 - Targets
 - Timing
 - Logistic constraints
 - Location of critical command-and-control nodes
- Mobilization
 - Intent to mobilize before public announcement
 - Impact on military-industrial base
 - Impact on civil economy
 - Transportation capabilities and limitations
- ISR
 - Purpose of collection
 - Targets of collection
 - Timing
 - Capabilities of collection assets
 - Processing capabilities
 - Unit requesting collection
- Peacetime weapons and other military movements
 - Fact of movement
 - Periodicity of movements
 - Origin and destination of equipment being moved
 - Capabilities and limitations of equipment being moved
 - Extent of inventory of equipment being moved
- Command-post or field-training exercises
 - Participating units
 - OPLAN, CONPLANs, or other contingencies that are being exercised
 - Command relationships
 - C4 connections and weaknesses
 - Logistic capabilities and limitations
- Non-combatant evacuation operations (hostile environment)
 - Targets
 - Forces
 - Logistic constraints
 - Safe havens
 - Routes
 - Timing
- Counterdrug operations
 - Identity of military forces
 - Law Enforcement Agency (LEA) involvement
 - Military support to LEAs

- Host-nation cooperation
- Capabilities
- Timing
- Tactics
- Logistic capabilities and constraints

For more information, see AR 380-5.

Appendix F

Examples of CUI

Various laws and executive orders require CUI to be protected. The following list contains examples of CUI but is not all-inclusive.

- Information concerning a protected person
- FOUO information (see Chapter 5, AR 380-5)
- Export-controlled technical data on the Military Critical Technologies List (as required by the Export Administration Act (50 USC App. 2401-2420) of 1979, extended by EO 13222 under the International Emergency Economic Powers Act)
- Sensitive information as defined in USC 15 278g-3(d)(4)/Public Law 100-235, the Computer Security Act of 1987
- Contract financial data in the pre-award stage
- Military operational and tactical information
- DoD-developed computer software
- Proprietary data (trade secrets), such as patent secrecy data or data obtained from a company on a confidential basis
- Test material used in an academic environment
- Law-enforcement-sensitive information
- Certain data compiled for law-enforcement purposes
- Confidential medical records
- Inter- and intra-agency memoranda that are deliberative in nature
- Employee personal data
- Internal rules and practices of a government agency that, if released, would circumvent an agency policy and impede the agency in the conduct of its mission

For more information, see AR 380-5.

Appendix G

Examples of FOUO information

The following examples illustrate types of FOUO information but are not an exclusive listing and are not intended to offer guidance in responding to FOIA requests.⁶¹⁰

- TRADOC EEFI
- PII except that of official, designated command spokespersons and/or GOs and GOs' civilian equivalents (SES)
 - PII about U.S. citizens, DoD employees, and military personnel, such as SSNs, dates of birth, home addresses, and telephone numbers other than duty office numbers. (However, duty phone numbers of units described in Paragraphs C.3.2.1.6.2.2. of DoD 5400.7-R may not be posted.)⁶¹¹
 - PII, including compilations of names of personnel assigned to overseas, sensitive, or routinely deployable units⁶¹²
 - Names, locations, and any other identifying information about family members of DoD employees and military personnel⁶¹³
 - Duty rosters or detailed organizational charts and directories with names (as opposed to organizational charts, directories, general telephone numbers for commonly requested resources, services, and contacts without names)
 - Official travel itineraries of individuals (both personal and official) and units before it is performed⁶¹⁴
- Confidential personal records
 - Financial records (12 USC §3403)
 - Medical records (10 USC §1102) and patient records (42 USC §290dd-2)
 - Financial disclosure reports of special government employees (5 USC App. 4, §207 (a) (1) 2)
 - Action on reports of selection boards (10 USC §618)
 - Drug-abuse prevention / rehabilitation records (21 USC §1175)
 - Information concerning U.S. personnel classified as prisoners of war (POW) / missing in action (MIA) during the Vietnam Conflict (42 USC §401)
- Information in files, the release of which would cause a clearly unwarranted invasion of personal privacy
 - Records compiled to evaluate or adjudicate the suitability of candidates for civilian employment or membership in the armed forces
 - The eligibility of civilian, military, and contractors for security clearances or access to particularly sensitive classified information
 - Reports, records, and other material pertaining to personnel matters in which administrative action, including disciplinary action, may be taken
 - Records containing PII such as SSNs, dates of birth, home addresses, home telephone numbers, personal email addresses
 - Evaluations of performance and performance counseling
 - Financial information included on timecards, leave-and-earning statements, and travel vouchers
 - Particularly sensitive, often graphic, details pertaining to an individual's death, including autopsy reports
- Specific force-protection measures
- Movement and readiness data

⁶¹⁰ Paragraph 3.5.3, Part II, DoD Web policy.

⁶¹¹ Paragraph 3.5.3.4, Part II, DoD Web policy.

⁶¹² Paragraph 3.5.3.3, Part II, DoD Web policy.

⁶¹³ Paragraphs 3.5.3.5, Part II, and 2.2, Part V, DoD Web policy.

⁶¹⁴ Paragraphs 5a(1) and 5a(2), TRADOC OPSEC Plan; Paragraph 2.2, Part V, DoD Web policy.

- Information protected by copyright
- Draft publications
- Information concerning security systems
 - Documentation (for example, maps, test, and evaluation results; vulnerability assessments; audits, results, or findings) describing operational information-system architectures, designs, configurations, vulnerabilities, address listings, or user information⁶¹⁵
 - Information that is a collection of interrelated processes, systems, and networks that provides information on information-assurance services throughout the Army, the AKM environment, or the incident detection and response infrastructure, capabilities, or configuration⁶¹⁶
- Internal DoD personnel rules and practices unless cleared for release to the public. This includes two “profiles”: high and low. “High” is information pertaining solely to the internal personnel rules and practices of the Army which, if released, could allow circumvention of a rule, policy, or statute, thereby impeding the Army in the conduct of its mission. “Low” is information permitted from withholding under the FOIA if there is no public interest in the document and it would be an administrative burden to process the FOIA request.
 - Operating rules, guidelines, and manuals for investigators, inspectors, auditors, or examiners that must remain privileged to fulfill a legal requirement
 - Personnel and other administrative matters, such as examination questions and answers used in training courses or in determining the qualification of candidates for employment, entrance on duty, advancement, or promotion
 - Computer software, the release of which would allow circumvention of a statute, rule, regulation, order, directive, or instruction
 - Installation or building vulnerability assessments
- Internal documents that are pre-decisional in nature and part of the decision-making process containing advice, subjective evaluations, opinions, and recommendations; also within the scope of this exemption are attorney-client and attorney work product privileged documents
 - Nonfactual portions of staff papers, to include after-action reports and situation reports containing staff evaluations, advice, opinions, or suggestions
 - Advice, suggestions, or evaluations prepared on behalf of the Army by individual consultants, board, committees, councils, groups, panels, conferences, commissions, task forces, or other groups formed for the purpose of obtaining advice and recommendations
 - Nonfactual portions of evaluations of contractors
 - Information of a speculative, tentative, or evaluative nature, or such matters as proposed plans to procure, lease, or otherwise acquire and dispose of materials, real estate, facilities, or functions, when such information would provide undue or unfair competitive advantage to private personal interests or would impede legitimate Army functions
 - Trade secrets or other confidential research development, or commercial information owned by the government, where premature release is likely to affect the government’s negotiating position or other commercial interests
 - Records that are exchanged among agency personnel as part of the preparation for anticipated litigation before any federal, state, or military court, or administrative proceeding by an agency, as well as records that qualify for the attorney-client privilege
 - Portions of official reports of inspection, audits, investigations, or surveys pertaining to safety, security, or other internal management, administration, or operation when the information has been treated by the courts as privileged against disclosure in litigation
 - Computer software that reveals policies, functions, decisions, or procedures which is deliberative in nature, the disclosure of which would inhibit or chill the decision-making process

⁶¹⁵ Paragraph 4-13, AR 25-2.

⁶¹⁶ Paragraph 4-13, AR 25-2.

- Computer models used to forecast budget outlays, calculate retirement costs, or optimize models on travel costs
 - Planning, programming, and budgetary information which is involved in the defense planning and resource-allocation process
- Specifically exempted from public disclosure by statute
 - Technical data packages
 - Certain sensitive information of foreign governments and international organizations
 - Research other than contracts and grants
 - National historic preservation (16 USC §470w-3)
 - Data sheets involving control of arms exports and imports
 - Contract proposal information (10 USC §2305 (g))
 - Pre-award protest document
 - Contract data subject to the Procurement Integrity Act
 - Representation rights and duties, labor unions (5 USC §7114 (b)(4))
 - Civil-service examination (18 USC §1917)
 - Confidential status of patent applications (35 USC §122)
 - Secrecy of certain inventions and withholding of patents (35 USC §181-188)
 - Confidential inventions information (35 USC §205)
 - Administrative dispute resolutions (5 USC §574 (j))
- Commercial / industry information
 - Trade secrets, commercial or financial information obtained from a person or organization outside the government on a privileged or confidential basis which, if publicly released, would result in competitive harm to the company, impair the Army's ability to obtain similar information in the future or harm some other legitimate government interest⁶¹⁷
 - Commercial or financial information received in confidence in connection with loans, bids, contracts, proposals, trade secrets, inventions, discoveries, or other proprietary data
 - Statistical data concerning contract performance, income, profits, losses, and expenditures if offered and received in confidence from a contractor or potential contractor
 - Personal statements given in the course of inspections, investigations, or audits that are received and retained in confidence and that contain trade secrets or information that is normally considered confidential or privileged
 - Financial data provided in confidence by private employers in connection with locality wage surveys
 - Scientific and manufacturing processes, developments, and other information concerning technical or scientific data and other information submitted with an application for research grant or with a report while research is in progress
 - Technical or scientific data developed by a contractor in whole or in part at private expense wherein the contractor has retained legitimate proprietary interests
 - Computer software that is copyrighted
 - Test and evaluation information that could result in an unfair advantage or disadvantage to the manufacturer or producer⁶¹⁸
 - Technical information not marked or otherwise determined to be appropriate for Distribution Statement A IAW DoDD 5230.24. This includes all technical information that can be used or be

⁶¹⁷ Paragraph 3.5.3.6, Part II, DoD Web policy.

⁶¹⁸ Paragraph 3.5.3.7, Part II, DoD Web policy.

- adapted for use to design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce any military or space equipment or technology concerning such equipment⁶¹⁹
- Proprietary information submitted by a contractor and protected by a Limited Rights Statement or other agreement, and trade secrets, commercial, and financial information submitted by an entity outside the government that considers the information to be protected from release to the public.⁶²⁰
 - Test and evaluation of commercial products or military hardware produced by a non-governmental entity
 - Patents, unless licensed for publication by the United States
 - Software documentation: shall be distributed according to the terms of the software license
 - Premature dissemination: the information related to patentable military systems or processes in the developmental stage
 - Compiled for law-enforcement purposes that could interfere with law-enforcement proceedings, deprive a person of a right to a fair trial, cause an unwarranted invasion of personal privacy, identify a confidential source, reveal investigative techniques and procedures, or endanger the life or physical safety of an individual
 - Records of agencies responsible for the supervision of financial institutions (generally not included with Army subject matter)
 - Geological and geophysical information and maps concerning wells (generally not included with Army subject matter)⁶²¹
 - Scientific and technological information relating to:
 - Critical technology on either the Munitions List or the Commerce Control List
 - Unclassified special nuclear weapons information (10 USC §128)
 - Unclassified technical data with military or space application (10 USC §130)
 - Centers for Industrial Technology – reports of technology innovations (15 USC §3705 (e)(E))
 - Information regarding atomic energy (42 USC §2161-2168)
 - Control of arms exports, Sec 38(e) of the Arms Export Control Act (22 USC §2778(e))
 - Technical and scientific data developed by a contractor or sub-contractor exclusively or in part at private expense
 - Weapon schematics
 - Weapon-system vulnerabilities
 - Electronic wire diagrams
 - Frequency-spectrum data
 - Scientific and technological information such as critical technology or nuclear weapons technology⁶²²
 - Sensitive science and technology reports⁶²³ such as:
 - Defense Acquisition Executive System reports
 - Selected acquisition reports
 - Weapons System Unit Cost reports
 - Approved program baselines for ACAT I, II, III weapons systems
 - Weapons systems evaluation and testing results and reports
 - Reports based on Joint U.S. and foreign government technical research and weapons-systems evaluations

⁶¹⁹ Paragraph 3.5.3.8, Part II, DoD Web policy.

⁶²⁰ Paragraph 3.5.3.6, Part II, DoD Web policy.

⁶²¹ Paragraph L-1i, Appendix L, AR 530-1.

⁶²² Paragraph 2.5, Part V, DoD Web policy.

⁶²³ Paragraph 2.5, Part V, DoD Web policy.

- Weapons-system contractor performance reporting under Earned Value Reporting System at the level of CPE reporting
 - Weapons-systems staff working papers, correspondence, and staff assessments
 - DoD component “feedback” staff working papers and assessments on weapons-system program performance
- Intelligence information relating to:⁶²⁴
 - Organizational and personnel information for Defense Intelligence Agency (DIA), NRO, and NIMA (10 USC §424)
 - Maps, charts, and geodetic data (10 USC §455)
 - Communications intelligence (18 USC §798)
 - NSA functions and information (50 USC §402)
 - Protection of identities of U.S. undercover intelligence officers, agents, informants and sources (50 USC §421)
 - Protection of intelligence sources and methods (50 USC §403(d)(3))
- Military operations
 - Analysis and recommendations concerning lessons-learned which would reveal sensitive military operations, exercises, or vulnerabilities⁶²⁵
 - Reference to unclassified information that would reveal sensitive movements of military assets or the location of units, installations, or personnel where uncertainty regarding location is an element of a military plan or program⁶²⁶

For more information, see AR 530-1, Chapter 5 of AR 380-5, and Paragraph 2, Part V, in the DoD Web policy.

⁶²⁴ Paragraph 2.6, Part V, DoD Web policy.

⁶²⁵ Paragraph 3.5.3.1, Part II, DoD Web policy.

⁶²⁶ Paragraphs 3.5.3.2, Part II, and 2.1, Part V, DoD Web policy.

Appendix H

Examples of OPSEC indicators

- Administration⁶²⁷
 - Temporary duty (TDY) orders
 - Attendance at planning conferences
 - Transportation arrangements
 - Billeting arrangements
 - Medical care
 - Schedules
 - Plans of the day
 - Exercise, deployment, training, or leave schedules for large groups or entire units
 - Increased family-support activities or family-support plans that may indicate impending deployment
 - Reserve mobilization
 - Changes to daily schedules
 - Notice to Airmen (NOTAM)
 - International Civil Aviation Organization (ICAO) notices
 - Change of mail addresses or arrangements to forward mail on a large scale
 - Runs on post exchange for personal articles – for example, personal radios
 - Emergency personnel requisitions and fills for critical skills
 - Emergency recall of personnel on leave and pass
- Operations, plans and training
 - Changes in defense readiness condition (DEFCON), force-protection condition (FPCON), or information condition (INFOCON)
 - Movement of forces into position for operations
 - Abnormal dispersions or concentrations of forces
 - Deviations from routine training
 - Rehearsals and drills for a particular mission
 - Exercises and training in particular areas with particular forces
 - Repeating operations the same way, same time, same route, or in same area. Fixed schedules and routes
 - Standard reactions to hostile acts
 - Standardizing maneuvers or procedures
 - Standardizing force mixes and numbers to execute particular missions down to squad-level operations
 - Changing guards at fixed times
 - Appearance of special-purpose units (for example, bridge companies, pathfinders, explosive-ordnance detachments (EOD), SOF, or liaison officer (LNO) teams)
 - Change in task organization or arrival of new attachments
 - Artillery registration in new objective area
 - Surge in food deliveries to planning staffs at major headquarters
 - Unit and equipment deployments from normal bases
- Communications

⁶²⁷ See Appendix D, AR 530-1.

- Voice and data (telephone, cellphone, wireless) transmissions between participants in an operation
 - Establishment of command nets
 - Spectrum emissions and associated documentation
 - Changes in activity or communications patterns
 - Changes in message volume (phone calls to secure systems), such as increased radio, email, and telephone traffic from headquarters
 - Units reporting to new commanders
 - Identification of units, tasks, or locations in unsecured transmissions
 - Increased communications checks between units / organizations
 - Unnecessary or unusual increase in reporting requirements
 - Sudden imposition of communications-security measures, such as radio silence
 - Appearance of new radio stations in a net
 - Communications exercises
 - Appearance of different cryptographic equipment or materials
 - Increase in unofficial use of commercial email services
 - Increased use of Internet and / or email such as special Webpages posted by unit personnel and/or more email traffic for personal or official business
 - Unofficial use of Instant Messenger, chat forums, or bulletin boards / messages between Soldiers and family members
- Intelligence, counterintelligence, and security
 - Concentrated reconnaissance in a particular area
 - Embarking or moving special equipment
 - Recruitment of personnel with particular language skills
 - Routes of reconnaissance vehicles
 - Sensor drops in target area
 - Increased activity of friendly agent nets
 - Increased ground patrols
 - Unusual or increased requests for meteorological or oceanographic information
 - Unique or highly visible security to load or guard special munitions or equipment
 - Adversary radar, sonar, or visual detection of friendly units
 - Friendly unit identifications through communications-security violation, physical observation of unit symbols, etc.
 - Trash and recycle bins that contain critical information
- Logistics
 - Volume and priority of requisitions
 - Package or container labels that show the name of an operation, program, or unit designation
 - Prepositioning equipment or supplies
 - Procedural disparities in requisitioning and handling
 - Accelerated maintenance of weapons and vehicles
 - Presence of technical representatives
 - Unusual equipment modification
 - Increased motorpool activities
 - Test equipment turnover
 - Special equipment issue
 - Stockpiling petroleum, oil, lubricants, and ammunition

- Upgraded LOCs
 - Delivery of special or uncommon munitions
 - New support contracts or host-nation agreements
 - Arranging for transportation and delivery support
 - Requisitions in unusual quantities to be filled by a particular date
- Engineer
 - New facility leases
 - Construction of mock-ups for special training
 - Production or requisitions of unusual amounts of maps and charts, or products for unusual areas
 - Attachment of specialized heavy equipment
- Medical
 - Stockpiling plasma and medical supplies
 - Movement of deployable medical sets (DEPMEDS)
 - Immunization of units with area specific and time-dependent vaccines
 - Identifying special medical personnel and teams deploying to specific areas
 - Sudden recall of National Guard and Army Reserve doctors to active duty
- Emissions other than communications
 - Radar and navigational aids that reveal location or identity
 - Normal lighting in a blackout area
 - Operating at unusual speed in water
 - Loud vehicle or personnel movements
 - Smoke and other odors
- RDT&E and acquisition activities
 - Solicitations for subcontractors to perform portions of the work
 - Lists of installations that are involved in particular contracts or projects
 - Specialized hiring of personnel for particular contracts or projects
 - Highlighting specific security needs or requirements for portions of a projector contract
 - Testing range schedules
 - Unencrypted emissions during tests and exercises
 - Public media, particularly technical journals
 - Budget data that provides insight into the objectives and scope of a system research-and-development effort or the sustainability of a fielded system
 - Deployment of unique units, targets, and sensor systems to support tests associated with particular equipment or systems
 - Unusual or visible security imposed on particular development efforts that highlight their significance
 - Special manning for tests or assembly of personnel with special skills from manufacturers known to be working on a particular contract
 - Stereotyped use of location, procedures, and sequences of actions when preparing for and executing test activity for specific types of equipment or systems
 - Advertisements indicating that a company has a contract on a classified system or component of a system, possesses technology of military significance, or has applied particular principles of physics and specific technologies to sensors and the guidance components of weapons
 - Schedules (delivery, personnel arrival, transportation, test, ordnance loading, etc.) posted where personnel without a need-to-know have access
 - Conferences, symposia, and internal professional forums

For more information, see Appendix D, AR 530-1, and Paragraph 2, Part V, of the DoD Web policy. Also see Paragraph 3, Appendix C, JP 3-54, for examples of OPSEC indicators.

Appendix I

Examples of sensitive information

- PII except that of official, designated command spokespersons and / or GOs and SESs
- Photographs
 - Results of IED strikes
 - Battle scenes
 - Casualties
 - Destroyed or damaged equipment
 - Personnel KIA, both friendly and adversary
 - Protective measures of military facilities⁶²⁸
 - C2 nodes
 - Installation photography⁶²⁹
 - Weapons-systems vulnerabilities
 - Friendly TTP
 - Photos that may have a negative impact on foreign relations with Coalition allies or on world opinion
 - Equipment vulnerabilities
 - Intelligence-collection efforts and methods
 - Ongoing friendly operations
- Other images
 - Detailed maps
 - Detailed organizational charts
- Proprietary information
 - Contractor proposals
 - Confidential commercial or financial information
- Documents and files
 - Pre-decisional documents
 - Information that must be protected under legal conditions such as the Privacy Act
 - Administration and personnel
 - Acquisition plans
 - Information in routine DoD payroll, finance, logistics, and personnel-management systems
- Army
 - Structure and manning
 - Equipment
 - Readiness
 - Mission-specific training
 - Funding
 - Sustainment
 - Deployments
 - Stationing
 - DoD / Army vulnerabilities

⁶²⁸ Paragraph 2-1c, AR 530-1.

⁶²⁹ Paragraph 2.1, Part V, DoD Web policy.

- DoD / Army present and future capabilities
 - Insights into national/military morale
- Intelligence, counterintelligence, and security
- Medical
- Casualties
- As described in the following categories:
 - FOUO – IAW DoD 5400.7-R, unclassified information that may be withheld from mandatory public disclosure under the FOIA;
 - Unclassified technical data – data related to military or dual-use technology that is subject to approval, licenses, or authorization under the Arms Export Control Act and withheld from public disclosure in accordance with DoD 5230.25;
 - DoS SBU – information originating from DoS that has been determined to be SBU under appropriate DoS information security policies;
 - Foreign government information – information originating from a foreign government that is not classified “confidential” or higher but must be protected IAW DoD 5200.1-R;
 - Privacy data – personal and private information (for example, individual medical information, home address and telephone number, SSN) as defined in the Privacy Act (see AR 340-21);
 - Special handling – unclassified information that requires special handling (for example, limited distribution, Encrypt For Transmission Only, and scientific and technical information protected under the Technology Transfer Laws and Arms Export Control Act);
 - CUI – see CUI entry in definitions section and Appendix F;
 - FOIA-exempt information – the FOIA specifies nine categories of information that can be withheld from release if requested by the public.
- Military planning, operations and exercises:
 - OPODs, OPLANs, CONOPs, and training information – these might reveal military operations, exercises, vulnerabilities, or state of unit readiness (for instance, unit-readiness-specific information is sensitive)
 - SOPs
 - Reference to unclassified information that would reveal sensitive movements of military assets or the location of units, installations or personnel where uncertainty regarding location is an element of a military plan or program⁶³⁰
 - TTP and Army lessons-learned, including after-action reports (AARs). Army lessons-learned is often a result of an AAR, and AARs contain specific information about TTP the Army uses to conduct operations. Lessons-learned also often include analysis and recommendations that would be adopted for current and future military operations and exercises.⁶³¹ Especially be alert to information related to emerging Operation Iraqi Freedom (OIF) / Operation Enduring Freedom (OEF) TTP, including (but not limited to), individual tasks, enemy TTP, countermeasures / counter-countermeasures, analysis, conclusions, and sequences of events
 - Planning guidance
 - Detailed budget reports
 - Inventory reports
 - Unit organization
 - Detailed mission statement
 - Specific unit phone / fax numbers (secure and unsecured)
 - Time-phase force-deployment data

⁶³⁰ Memorandum from the DEPSECDEF, “Information Vulnerability and the Worldwide Web,” Sept. 24, 1998; Paragraphs 3.5.3.2, Part II, and 2.1, Part V, DoD Web policy.

⁶³¹ Paragraph 3.5.3.1, Part II, DoD Web policy.

- Ops schedules
- Logistics support requirements
 - Medical
 - Civil engineering
 - Petroleum, oil, lubricants (POL)
 - Host-nation support
 - Transportation
 - Munitions
- Force apportionment
- Force allocation
- Unit bed-down information
- Unit augmentation
- Force synchronization
 - Unit shortfalls
- Counter-terrorism information
- ISR capabilities
- C4I architecture
- Non-combatant evacuation operations (NEO) plans or ops
- Counter-drugs ops
- Unit recall rosters
- Unit relocations / deployments
- Weapons movements
- Mobilization information
- Communications methods
- Critical maintenance
- Exercise and simulations activity
- Inspection results, findings or deficiencies
- Unit vulnerabilities or weaknesses
- Test and evaluation information – could result in an unfair advantage or disadvantage to the manufacturer or producer or could reveal the capabilities, limitations or incapacities of a DoD weapons systems or component
- Information relating to A-76 studies and other outsourcing studies that provide detailed descriptions of sensitive organizational operations⁶³²

For more information, see Paragraph 2, Part V, DoD Web policy.

⁶³² Paragraph 2.7, Part V, DoD Web policy.

Appendix J

Consolidated list of PII

A number of documents identify PII, which is generally prohibited on the publicly accessible Web unless for an official, designated command spokesperson and / or a GO or SES. (And in those cases, their marital status and family-member information is prohibited.) PII includes, but is not limited to, the following individual and collective (group) categories:

- Name;⁶³³
- Date of birth;⁶³⁴
- Place of birth;⁶³⁵
- Age;⁶³⁶
- Home address;⁶³⁷
- Race;⁶³⁸
- Email address containing personal name;⁶³⁹
- SSN;⁶⁴⁰
- Marital status;⁶⁴¹
- Names, locations, and any other identifying information about family members of DoD employees and military personnel,⁶⁴² including family-member information within permitted biographies;⁶⁴³
- Biographies of people who are not official, designated command spokespersons;⁶⁴⁴
- Photographs of personnel;⁶⁴⁵
- Description of personnel;⁶⁴⁶
- Personal daily or travel schedules;⁶⁴⁷
- Military rank;⁶⁴⁸

⁶³³ Enclosure 2, DoDD 5400.11; OMB M-07-16. DoD broadened what PII is FOIA-exempt to include lists of DoD personnel, anything that verifies the status of individuals, or names in documents that do not fall into these categories in the OSD memorandum, “Withholding of Personally Identifying Information Under the Freedom of Information Act (FOIA),” Nov. 9, 2001. See also memorandum from the ASD-C3I, “Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites,” Dec. 28, 2001.

⁶³⁴ Enclosure 2, DoDD 5400.11; Paragraph 2.2, Part V, DoD Web policy; memorandum from the DEPSECDEF, “Information Vulnerability and the Worldwide Web,” Sept. 24, 1998.

⁶³⁵ Enclosure 2, DoDD 5400.11.

⁶³⁶ Ibid.

⁶³⁷ Enclosure 2, DoDD 5400.11; Paragraph 2.2, Part V, DoD Web policy; memorandum from the DEPSECDEF, “Information Vulnerability and the Worldwide Web,” Sept. 24, 1998.

⁶³⁸ Enclosure 2, DoDD 5400.11.

⁶³⁹ Part III, DoD Web policy; memorandum from ASD-C3I, “Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites,” Dec. 28, 2001.

⁶⁴⁰ Enclosure 2, DoDD 5400.11; Paragraph 2.2, Part V, DoD Web policy; memorandum from ASD-C3I, “Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites,” Dec. 28, 2001; DEPSECDEF memorandum, “Information Vulnerability and the Worldwide Web,” Sept. 24, 1998.

⁶⁴¹ Enclosure 2, DoDD 5400.11.

⁶⁴² Paragraph 2.2, Part V, DoD Web policy; memorandum from ASD-C3I, “Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites,” Dec. 28, 2001; DEPSECDEF memorandum, “Information Vulnerability and the Worldwide Web,” Sept. 24, 1998.

⁶⁴³ See definitions section for *family member*.

⁶⁴⁴ Memorandum from ASD-C3I, “Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites,” Dec. 28, 2001; key management control list, Appendix C, AR 25-1; TRADOC Command Guidance: Noble Eagle #02-019, “Personal Data on Unclassified Websites,” March 13, 2002.

⁶⁴⁵ Ibid.

⁶⁴⁶ Enclosure 2, DoDD 5400.11.

⁶⁴⁷ From Army Web content and OPSEC training module, <https://iatraining.us.army.mil>.

- Civilian grade;⁶⁴⁹
- Official title;⁶⁵⁰
- Salary / pay information;⁶⁵¹
- Telephone numbers other than numbers of duty offices;⁶⁵²
- Medical information;⁶⁵³
- Mother's maiden name;⁶⁵⁴
- Biometric records;⁶⁵⁵
- Rosters / lists of names;⁶⁵⁶
- Directories, including telephone directories, with names;⁶⁵⁷
- Charts with names;⁶⁵⁸
- Unit recall rosters;⁶⁵⁹
- Detailed duty rosters with names.⁶⁶⁰

⁶⁴⁸ Enclosure 2, DoDD 5400.11; memorandum from ASD-C3I, "Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites," Dec. 28, 2001; memorandum from OSD, "Withholding of Personally Identifying Information Under the Freedom of Information Act (FOIA)," Nov. 9, 2001.

⁶⁴⁹ Enclosure 2, DoDD 5400.11.

⁶⁵⁰ Memorandum from OSD, "Withholding of Personally Identifying Information Under the Freedom of Information Act (FOIA)," Nov. 9, 2001.

⁶⁵¹ Enclosure 2, DoDD 5400.11; memorandum from OSD, "Withholding of Personally Identifying Information Under the Freedom of Information Act (FOIA)," Nov. 9, 2001.

⁶⁵² Paragraph 2.2, Part V, DoD Web policy; memorandum from the DEPSECDEF, "Information Vulnerability and the Worldwide Web," Sept. 24, 1998. However, Enclosure 2, DoDD 5400.11, lists "office phone number" as an example of PII.

⁶⁵³ Enclosure 2, DoDD 5400.11.

⁶⁵⁴ Enclosure 2, DoDD 5400.11; OMB M-07-16.

⁶⁵⁵ Ibid.

⁶⁵⁶ Paragraph 2.2, Part V, DoD Web policy; memorandum from ASD-C3I, "Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites," Dec. 28, 2001.

⁶⁵⁷ Paragraph 2.2, Part V, DoD Web policy; memorandum from ASD-C3I, "Removal of Personally Identifying Information of DoD Personnel from Unclassified Websites," Dec. 28, 2001.

⁶⁵⁸ Ibid.

⁶⁵⁹ Paragraph 2.1, Part V, DoD Web policy.

⁶⁶⁰ From Army Web content and OPSEC training module, <https://iatraining.us.army.mil>.

Appendix K

Information-posting process (DoD requirements)

Following is the information-posting process IAW DoD's requirement described in Paragraph 2, Part V, of the DoD Web policy, which states that "[a]ll information proposed for posting to a publicly accessible Website must be reviewed [IAW] the provisions of [DoDD] 5230.9 and [DoDI] 5230.29, and as described in Paragraph 3, Part II, of [the DoD Web policy]." Information in brackets and / or brown type below is Army or TRADOC additions to the DoD Web policy, introduced for clarification.

PARAGRAPH 3, PART II, DOD WEB POLICY

Those who establish Websites are responsible for instituting a process to identify information appropriate for posting to those Websites, and the appropriate security and access controls. The steps of this process are:

1. Identification of information that needs to be conveyed quickly and efficiently and thus will benefit from the attributes of the Web;
2. Identification of a specific target audience for the information;
3. Identification of the DoD originating office (DOO) for the information if the sensitivity of the information or distribution restrictions on its release cannot be readily ascertained;
4. Review of the content for sensitivity and distribution / release controls, including sensitivity of information in the aggregate;
5. Determination of the appropriate access and security controls;
6. Approval of the information for public release IAW DoDD 5230.9 and DoDI 5230.29 if it is to be posted to a publicly accessible Website [because the news media uses DoD Websites to gather information, DoDD 5122.5 and DoDI 5400.13 also apply];
7. Posting the information, once all required steps have been taken;
8. Verification; and
9. Feedback reporting, including "lessons learned."

More information on each step follows.

Step 1, identify information. The WWW provides DoD with a powerful tool to convey suitable information quickly and efficiently on a broad range of topics relating to its activities, objectives, policies, and programs. It is at the heart of the Defense Reform Initiative and is key to re-engineering and streamlining DoD's business practices. The American democratic process rests on the right of our citizens to know what their government is doing and the corresponding ability to judge its performance. Access to information by the public through the Web is an important component of this right. Nevertheless, careful examination of the potential consequences of placing information on the Web must be undertaken before it is made available. [For instance, OPSEC must be assessed before information is disseminated.]

Identifying information [that has a valid mission need to be posted] to the Web will normally be made by the entity that generates the information and thus has the best knowledge of its content.

Step 2, identify target audience. Illustration 2, Part II of the DoD Web policy, depicts many of the target audiences for DoD information posted to the Web. (Target audiences are also discussed in Chapter 4 of this *Guide*.) Only information of value to the general public and which does not require additional protection should be posted to publicly accessible sites on the WWW. Information requiring additional protection, such as FOUO information, information not specifically cleared and approved for public release, or information of questionable value to the general public and for which worldwide dissemination poses an unacceptable risk to the DoD, including military personnel and civilian employees, should be placed on Websites with security and access controls.

Step 3, identify DOO. The DOO is the entity that created or sponsored the work that generated the information or received / acquired the information on behalf of DoD. The DOO has the responsibility for assigning appropriate markings to information to include its sensitivity (for example, classified, FOUO, or other distribution-control markings for unclassified information), its releasability to the public [at TRADOC, this is done in conjunction with the PAO], and the approved audience for access (for example, DoD only, contractors, general public, etc.). The

DOO shall be consulted whenever there is doubt with regard to the sensitivity of the information or distribution restrictions on its release.

Step 4, review content. Organizational heads must establish, IAW DoDD 5230.9 and DoDI 5230.29, clearance-review procedures for official DoD information that is prepared by or for DoD personnel and is proposed for posting to publicly accessible Websites. Review procedures must address the need for trained and knowledgeable personnel, familiar with the rules governing FOUO information as well as pertinent SCGs, as appropriate. These individuals must also be familiar with the aspects of the organization's operations considered critical, its vulnerabilities, as well as the pertinent threat to assess the nature of the risk associated with posting specific information to Websites. This risk assessment must also include the increased sensitivity of certain information when electronically aggregated in significant volume.

In assessing the increased sensitivity that information may assume in electronic format, it is necessary to take into account the attributes of data mining (the nontrivial extraction of implicit, previously unknown, and potentially useful information from data). Data mining uses machine learning, statistical, and visualization techniques to discover and present knowledge in a form which is easily comprehensible to humans.

The content provider will also take into account the form in which the information is distributed, such as press releases, press conferences, or publicly disseminated documents, the susceptibility of the information to data mining, and the likelihood that the information could directly lead to the discovery and presentment of knowledge that is otherwise controlled (for example, classified information or FOUO information). [At TRADOC, this responsibility is in the hands of the organizational OPSEC officer and the content provider.] Also to be assessed is a specific risk to DoD's credibility if publicly released information is omitted and / or deleted from the Web. [This is determined by the PAO in TRADOC, in conference with the content provider.]

If the overall risk resulting from posting the information is determined to be unacceptable, the information must be given security and access controls. Part V of the DoD Web policy provides additional guidance in this area, while the paragraphs below provide specific prohibitions.

FOUO. Information, the disclosure of which would cause a foreseeable harm to an interest protected by one or more of the exemptions to the FOIA, shall not be posted to a publicly accessible Website. This information is designated FOUO pursuant to DoD 5400.7-R. While records containing FOUO information will normally be marked at the time of their creation, records that do not bear such markings shall not be assumed to contain no FOUO information without examination for the presence of information that requires continued protection and qualifies as exempt from public release. This may require coordination with the DOO for the information.

The following examples are illustrative of the type of information that may be considered as FOUO. These examples are not an exclusive listing, and they are not intended to offer any guidance in responding to FOIA requests. (Appendix G has a more extensive list, including the following but also drawn from other sources; the following list is specific to the DoD Web policy.)

- Analysis and recommendations concerning lessons-learned which would reveal sensitive military operations, exercises, or vulnerabilities.
- Reference to unclassified information that would reveal sensitive movements of military assets or the location of units, installations, or personnel where uncertainty regarding location is an element of a military plan or program.
- Personal information, including compilations of names of personnel assigned to overseas, sensitive, or routinely deployable units.
- Information, the release of which would be a clearly unwarranted invasion of personal privacy, to include the following categories about U.S. citizens, DoD employees and military personnel: 1) SSNs; 2) dates of birth; 3) home addresses; and 4) telephone numbers other than duty office numbers. Duty phone numbers of units described in Paragraphs C.3.2.1.6.2.2. of DoD 5400.7-R may not be posted.
- Names, locations, and specific identifying information about family members of DoD employees and military personnel.
- Proprietary information submitted by a contractor and protected by a Limited Rights Statement or other agreement, and trade secrets, commercial, and financial information submitted by an entity outside the government which considers the information to be protected from release to the public.

- Test and evaluation information that could result in an unfair advantage or disadvantage to the manufacturer or producer.
- Technical information not marked or otherwise determined to be appropriate for Distribution Statement A IAW DoDD 5230.24. This includes all technical information that can be used or be adapted for use to design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce any military or space equipment or technology concerning such equipment.

Unclassified information pertaining to classified programs. The clearance-review procedures for unclassified information pertaining to classified programs proposed for posting to publicly accessible Websites must take into account the likelihood of classification by compilation. Consultation with the program SCG may be required to determine the likelihood that the information – if compiled or aggregated with other information likely to be contained on publicly accessible Websites – will reveal an additional association or relationship that meets the standards for classification under DoD 5200.1-R. If such information is posted to a Website, it must be afforded security and access controls as specified in Part V [Table 1] of the DoD Web policy.

In instances where a question arises as to whether information in compilation / aggregation requires protection as classified information, and the information has not yet been posted on the Website, the DOO(s) for the information shall be contacted to obtain a decision before the information is posted. Where the information has already been posted, the information will be withdrawn from the system and will not be reposted until a decision is obtained from the DOO(s) for the information. In instances where there is a conflict among the DOOs as to the sensitivity of the information, which they are unable to resolve, the matter may be referred to the next higher level within each of the DOOs' organizations until a resolution can be obtained.

Users of a Website who believe that information on it, in compilation or aggregation, contains classified information should contact the webmaster of the system in question or, if the webmaster is unknown, report the matter to their own organization's security office for evaluation and action as appropriate.

When reviewers conduct multidisciplinary security assessments of Websites, advanced search engines (high-end natural-language-based systems optimized for English syntax analysis) and other automated means will be used to assess the likelihood of the presence of information classified by compilation.

Copyrighted material. Copyrighted material will be used only when allowed by prevailing copyright laws and may be used only if the materials relate to the organization's mission. Consult legal counsel when using any copyrighted material.

Conflicts of interest. IAW the JER, product endorsements or preferential treatment of any private organization or individual shall not appear on any official DoD publicly accessible site.

Step 5, determine access controls. A DoD Website may not post FOUO information, or information not specifically cleared and approved for public release, unless the information employs adequate security and access controls. Information of questionable value to the general public must be evaluated before worldwide dissemination to assess the risk to DoD. Adequate security and access controls must likewise be employed for such information if it is determined to place national security, DoD personnel and assets, mission effectiveness, or the privacy of individuals at an unacceptable level of risk.

Determinations as to the appropriate security and access controls to employ will be based upon the sensitivity of the information, the target audience for which the information is intended, and the level of risks to DoD interests. Part V [especially Table 1] of the DoD Web policy contains additional guidance.

Publicly accessible DoD Websites will not normally contain links or references to DoD Websites with security and access controls. Under certain circumstances, however, it may be appropriate to establish a link to a log-on site provided details as to the controlled site's contents are not revealed.

Step 6, approve release. Approval for posting information to publicly accessible Websites must be IAW the provisions of DoDD 5230.9 and DoDI 5230.29. (DoDD 5230.9 provides general guidance on clearing information that pertains to military matters, national-security issues, or subjects of significant concern to DoD; DoDI 5230.29 contains more specific instruction on what categories of information are included in "military matters, national-security issues, or subjects of significant concern to DoD.") Clearance / approval can be granted only by an appropriately trained individual specifically delegated that authority by the head of the DoD component or his / her designee. [Normally this is PAO as the commander's representative and spokesperson. However, DoDD 5230.9

does not apply to release of official DoD information to the news media⁶⁶¹ – that is governed by DoDD 5122.5 – and since the news media gather information from DoD Websites, the security and policy review process must also include coordination with Public Affairs. At TRADOC, this final approval for Website posting is done by PAO as the appropriate entity, in conjunction with security (OPSEC and / or G-2) and policy (G-6) SMEs. More details on the provisions of DoDD 5230.9 and DoDI 5230.29 follow.]

Step 7, post information. Once the procedures established in the preceding paragraphs have been completed, the information may be posted to the Web. In addition, the following steps must be accomplished.

Step 8, validate / verify information and links. A reasonable effort must be made to validate the information's accuracy. All links associated with the Website must be validated. IAW Paragraph 4.2, Part II, in the DoD Web policy, procedures must be established for each Website to ensure that:

- A comprehensive, multi-disciplinary security assessment addressing both content and technical issues is conducted at least annually;
- Periodic reviews are conducted to assess compliance with established information-posting procedures; and
- Outdated or superseded information is identified and promptly removed from the system or is appropriately archived.

Step 9, report feedback. Organizations may use tools such as Web statistics for user feedback. Since organizations must conduct an annual assessment and survey, they will likely find the annual assessment to be the most useful tool in gathering feedback. Further, IAW Paragraph 4.3, Part II, in the DoD Web policy:

- Reserve Component assets used for DoD-wide OPSEC and threat assessment of unclassified DoD Websites will observe feedback reporting, to include lessons learned.
- Website content providers and administrators will support and participate in the feedback reporting system. (See Appendix O.)
- Website content providers and administrators will review lessons learned and incorporate content and security changes where appropriate.

DODD 5230.9

This DoD directive specifies policy and responsibilities for the security and policy review process in clearing official DoD information proposed for official public release by DoD and its employees under DoDD 5105.2, *Deputy Secretary of Defense*. As a DoD directive, it applies to OSD, the military departments, offices of the CJCS and Joint Staff, the combatant commands, the defense agencies, DoD field activities, and all other organizational entities within DoD – collectively, these entities are called the DoD components – and all DoD personnel.

For provisions governing review of:

- Prepared statements, transcripts of testimony, questions for the record, inserts for the record, budget documents, and other material provided to congressional committees that may be included in published records – see DoDD 5400.4, *Provision of Information to Congress*.
- Information before publication or disclosure by DoD contractors – see DoD 5220.22-M, *National Industrial Security Program Operating Manual*, and DoD 5200.1-R, *Information Security Program Regulation*.
- Official information in litigation – see DoDD 5405.2, *Release of Official Information in Litigation and Testimony of DoD Personnel as Witnesses*.
- Release of official DoD information to the news media – see DoDD 5122.5, *Assistant Secretary of Defense for Public Affairs (ASD(PA))*.

DoD policy. It is DoD policy that:

- Accurate and timely information is made available to the public and Congress to help the analysis and understanding of defense strategy, defense policy, and national-security issues.

⁶⁶¹ Paragraph 2b(4), DoDD 5230.9.

- Any official DoD information intended for public release that pertains to military matters, national-security issues, or subjects of significant concern to DoD shall be reviewed for clearance prior to release. (See DoDI 5230.29 for more details on what types of information this includes.)
- The public release of official DoD information is limited only as necessary to safeguard information requiring protection in the interest of national security or other legitimate governmental interest, as authorized by DoD 5200.1-R, DoDD 5405.2, DoDD 5122.5, DoDD 5200.1 (*DoD Information Security Program*), DoDD 5230.24 (*Distribution Statements on Technical Documents*), DoDD 5230.25 (*Withholding of Unclassified Technical Data from Public Disclosure*), DoDI 5230.27 (*Presentation of DoD-Related Scientific and Technical Papers at Meetings*), DoDD 5400.7 (*DoD Freedom of Information Act Program*), DoD 5400.7-R (*DoD Freedom of Information Act Program (FOIA)*), DoDD 5400.11 (*Department of Defense Privacy Program*), DoD 5400.11-R (*Department of Defense Privacy Program*), DoDD 5205.2 (*DoD Operations Security Program*), DoDD 5500.7 (*Standards of Conduct*), DoD 5500.7-R (*Joint Ethics Regulation (JER)*), ITAR, EO 12958 (*Classified National Security Information*) as amended, Section 4353 of Title 22, U.S. Code, and presidential memorandum “Designation and Sharing of Controlled Unclassified Information,” May 9, 2008.
- Information released officially is consistent with established national and DoD policies and programs, including the DEPSECDEF memorandum “Ensuring Quality of Information Disseminated to the Public by the Department of Defense,” Feb. 10, 2003.
- To ensure a climate of academic freedom and to encourage intellectual expression, students (including midshipmen and cadets) and faculty members (DoD civilian or military) of an academy, college, university, or DoD school are not required to submit for review papers or materials that are prepared in response to academic requirements when they are not intended for release outside the academic institution. Information intended for public release or made available in libraries to which the public has access shall be submitted for review. Clearance shall be granted if:
 - Classified information is not disclosed;
 - DoD interests in are not jeopardized; and
 - The author accurately portrays official policy, even if the author takes issue with that policy.⁶⁶²
- Retired personnel, former DoD employees, and non-active-duty members of the Reserve Component shall use the DoD security-review process to ensure that information they submit for public release does not compromise national security.⁶⁶³
- DoD personnel, while acting in a private capacity and not in connection with their official duties, have the right to prepare information for public release through non-DoD forums or media. This information must be reviewed for clearance if it meets the criteria in DoDI 5230.29. Such activity must comply with ethical standards in DoDD 5500.7 and DoD 5500.7-R (the standards of conduct and JER) and may not have an adverse effect on duty performance or DoD’s authorized functions.

Responsibilities. The director, DoD Administration and Management (DA&M), acts as the appellate authority for the DoD security-review process.

The director, Washington Headquarters Services (WHS) – under the DA&M’s authority, direction and control – monitors compliance with DoDD 5230.9; develops procedures and review guidelines for the security and policy review of information intended for public release in coordination with offices of the OSD principal staff assistants; and implements the DoD security-review process through the OSR.

The heads of the DoD components:

- Provide prompt guidance and assistance to the WHS director, when requested, for the security or policy implications of information proposed for public release.
- Establish policies and procedures to implement DoDD 5230.9 in their components. Designate the DoD component office and point of contact for implementation of DoDD 5230.9 and provide this information to the OSR.

⁶⁶² Also in Paragraph 6-8c, AR 360-1.

⁶⁶³ Also in Paragraph 6-8g, AR 360-1.

- Forward official DoD information proposed for public release to the WHS director for review, including a recommendation on the releasability of the information, IAW DoDI 5230.29.

DODI 5230.29

This instruction implements the policy in DoDD 5230.9, assigns responsibilities, and prescribes procedures to carry out security and policy review of DoD information for public release IAW the authority in DoDD 5105.53. This DoDI applies to the DoD components.

It is DoD policy that, as specified in DoDD 5230.9, a security and policy review shall be done on all official DoD information intended for public release that pertains to military matters, national-security issues, or subjects of significant concern to DoD.

Responsibilities of organizations.

DA&M acts as the appellate authority for the DoD security-review process.

WHS.

- Monitors compliance with procedures established in Enclosure 3 of the DoDI for the security and policy review of official DoD information.
- Provides prompt security and policy review of official DoD information proposed for public release that is originated by, in, or for DoD, to include statements intended for open presentation before the Congress and other material submitted to Congress IAW DoDD 5400.4. The review is made to ensure that (1) properly classified information, (2) CUI, or (3) unclassified information that may individually or in aggregate lead to the compromise of classified information is not disclosed, and that no conflict exists with established policies or programs of DoD or the U.S. government.
- Provides prompt policy review of official DoD information that is originated by DoD for presentation before a closed session of Congress and other classified material submitted to Congress IAW DoDD 5400.4.
- Coordinates, as necessary, with the staffs of the DoD components when reviewing official DoD information for public-release clearance to ensure accuracy and currency of existing policy and security guidance.
- Responds to requests for review of information submitted voluntarily by non-DoD sources or DoD personnel acting in a private capacity to ensure that properly classified information is not disclosed. This review shall also address technology transfer and public releasability of technical data under DoDDs 5230.24 and 5230.25, and the ITAR.

DoD's general counsel conducts legal reviews, as needed, to ensure compliance with applicable laws and regulations to protect DoD rights and interests.

DoD components.

- Ensure compliance with DoDI 5230.29 and issue any guidance necessary for the internal administration of the requirements prescribed in Enclosure 3 of the DoDI.
- Forward official DoD information specified under Section 1 of the DoDI's Enclosure 3 that is proposed for public release to the OSR for review and clearance, as prescribed in Section 2 of the DoDI's Enclosure 3, with specific recommendations on the releasability of the information being forwarded.
- Provide prompt guidance and assistance to the OSR, when requested, on any information proposed for public release.
- Exercise clearance authority for information not specified in Enclosure 3 of DoDI 5230.29. This authority may be delegated to the lowest level competent to evaluate the content and implications of public release of the information.
- Review agency-specific documents internally. Ensure that information not specified in Enclosure 3 of DoDI 5230.29 is reviewed for OPSEC and INFOSEC IAW DoDD 5205.02 and DoD 5200.1-R prior to public release.
- Ensure compliance with the guidelines of the DEPSECDEF's memorandum, "Congressional Testimony Coordination and Clearance Procedures," March 3, 2007 (available at <http://www.dtic.mil/whs/esd/osr>),

concerning the coordination and clearance process of Congressional testimony to facilitate timely security and policy review.

- Ensure effective information-sharing with designated mission partners IAW DoDI 2205.02 and DoDD 3000.05.
- Ensure release of DoD information to news-media representatives is IAW DoDD 5122.5.

Procedures.

Clearance requirements (the following bullets equate to Section 1, Enclosure 3, of the DoDI) – Official DoD information that is prepared by or for DoD personnel and is proposed for public release shall be submitted (to the Chief, OSR, 1155 Defense Pentagon, Washington, D.C., 20301-1155) for review and clearance, *if* the information:

- Originates or is proposed for release in the National Capitol Region by senior personnel (e.g., flag officers and SES) on sensitive political or military topics;
- Is or has the potential to become an item of national or international interest;
- Affects national-security policy, foreign relations, or ongoing negotiations;
- Concerns a subject of potential controversy among the DoD components or with other federal agencies;
- Is presented by a DoD employee, who by virtue of rank, position, or expertise would be considered an official DoD spokesperson;
- Contains technical data, including data developed under contract or independently developed and controlled by the ITAR, that may be militarily critical and subject to limited distribution, but on which a distribution determination has not been made; or
- Bears on any of these critical topics (submit for review if proposed information addresses any of the following subjects or affects the OPSEC thereof):
 - New weapons or weapons systems, or significant modifications or improvements to existing weapons or weapons systems, equipment, or techniques.
 - Military operations and significant exercises of national or international significance.
 - C4I, IO, weapons of mass destruction, IEDs, and COMPUSEC.
 - Military activities or application in space; nuclear weapons, including nuclear weapons-effects research; chemical warfare and defensive biological warfare; initial fixed-weapons basing; and arms-control treaty implementation.
 - Any other contemporary topic that is designated by the head of a DoD component.

Submission for review (the following bullets equate to Section 2, Enclosure 3, of the DoDI) – The following procedures apply to all information required to be submitted to OSR for clearance:

- Paper submissions of packages – A minimum of three copies of the material, in its final form, shall be submitted, together with a signed DD Form 1910, “Clearance Request for Public Release of Department of Defense Information,” to OSR.
- Electronic submissions of packages – One soft copy of the material, in its final form (Microsoft Word), shall be submitted, together with a signed DD Form 1910, by email to secrev1@whs.mil.
- Material submitted for review shall be approved by the DoD component’s head or an authorized representative as may be delegated in writing to indicate approval of the material proposed for public release.
- All information submitted for review to OSR must first be coordinated within the originating DoD component to ensure that it reflects the organization’s policy position; does not contain classified information, CUI, or critical information requiring withholding; and is reviewed for OPSEC IAW DoDD 5205.02 and DoD 5200-R.

- Only the full and final text of material proposed for release shall be submitted for review. Notes, outlines, briefing charts, etc., may not be submitted as a substitute for a complete text. OSR reserves the right to return draft or incomplete documents without action.⁶⁶⁴
- Abstracts to be published in advance of a complete paper, manuscript, etc., require clearance. Clearance of an abstract does not fulfill the requirement to submit the full text for clearance before its publication. If an abstract is cleared in advance, that fact, and the OSR case number assigned to the abstract, shall be noted on the DD Form 1910 or other transmittal when the full text is submitted.⁶⁶⁵
- The requirements of DoDD 5400.4 and the DEPSECDEF's memorandum on congressional testimony (listed above) will apply to the processing of information proposed for submission to Congress.
- Information intended for placement on Websites or other publicly accessible computer servers (available to anyone without access controls) requires review and clearance for public release if it meets the requirements of Paragraph 1, Enclosure 3, in the DoDI. (See the list above in the "clearance requirements" subsection.) Website clearance questions should be directed to the component's Website manager. [In TRADOC, that would be the Website-content manager.] Review and clearance for public release is not required for information to be placed on DoD Websites or computer servers that restrict access to authorized users.
- Content submitters shall comply with DoD guidance on basic scientific and technical research review in DoDI 5230.27.

Time limits. Regular security and policy review requests:

- Submit speeches and briefings to OSR at least five working days before the event at which they are to be presented. More time may be needed for complex or potentially controversial speeches due to coordination requirements.
- Other material (e.g., papers and articles) shall be submitted to OSR at least 10 working days before the date needed. The length, complexity, and content shall determine the number of reviewing agencies and, consequently, the time required for the complete review process.
- Technical papers shall be submitted to OSR at least 15 working days before the date needed. More time may be needed if the material is complex or requires review by agencies outside DoD.
- Manuscripts and books shall be submitted to OSR at least 30 working days before the date needed. More time may be needed if the material is complex or requires review by agencies outside DoD.

Congressional security and policy review requests – security and policy review of material submitted by DoD to Congress will be provided to OSR in the following timeframes to allow for a thorough review to honor DoD's commitment to meet congressional committee or subcommittee mandates:

- Statements – five days before submission to the DoD Office of Legislative Counsel IAW Paragraph 2.2.2 in DoDD 5400.4 and the DEPSECDEF's memo on congressional testimony.
- Transcripts and the following related items – minimum of five working days: questions for the record, inserts for the record, advance policy questions, selected acquisition reports, budget documents (IAW Paragraph E1.3.4 of DoDD 5400.4).

Review determinations and appeals. Information reviewed for public-release clearance shall result in one of the following determinations:

- *Cleared for public release* – The information may be released without restriction by the originating component or its authorized official. OSR may require a disclaimer to accompany the information as follows: "The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. government."
- *Cleared "with recommendations" for public release* – Optional corrections, deletions, or additions are included. Although OSR has no responsibility for correcting errors of fact or making editorial changes,

⁶⁶⁴ Paragraph 6-8f, AR 360-1, is similar: "Notes, abstracts or manuscript/speech outlines will not be cleared as a substitute for the complete text, but may be reviewed unofficially as a courtesy. However, abstracts to be published in advance require clearance. An abstract clearance does not substitute for clearance requirements for the full and final text manuscript."

⁶⁶⁵ Ibid.

obvious errors may be identified in the text and noted as “recommended.” These corrections are not binding on the author or submitter.

- *Cleared “as amended” for public release* – Amendments, made in red, are binding on the submitter. Red brackets identify information that must be deleted. If the amendments are not adopted, then the DoD clearance is void. When possible, alternative wording is provided to substitute for the deleted material. Occasionally, wording will be included that shall be added to the text before public release. A disclaimer, as shown above, may also be required.
- *Not cleared for public release* – The information submitted for review may not be released.

All amendments or “not cleared” determinations may be appealed through OSR to the DA&M. All appeals shall be resolved at the lowest practical level and as quickly as possible.

Clarifications on the submission process to OSR. Information matching the categories of Section 1, Enclosure 3, of DoDI 5230.29 and of Paragraph 5-3a in AR 360-1, and intended for placement in public areas – such as on electronic bulletin boards accessible through the Internet or publicly accessible Webpages – must be submitted for security review⁶⁶⁶ to OSR in coordination with TRADOC PAO before the information is disseminated. The organization forwarding the information to OSR must include a recommendation on the releasability of the information to TRADOC PAO, who will include that recommendation in the submission to OSR. Since the OPSEC review must be conducted before submission to OSR, the OPSEC reviewer’s recommendation will be included in the overall recommendation on the information’s releasability.

IAW DoDI 5230.29, if the category of information is not specified in the list of Enclosure 3, the head of the DoD component is the clearance authority, but he / she may delegate that authority “to the lowest level competent to evaluate the content and implications of public release of the information.”⁶⁶⁷ At TRADOC, this clearance authority is PAO for all information intended for release into the public domain, unless the intended public release of information is specific to a FOIA request – then the TRADOC FOIA officer may be involved. Consult TRADOC PAO if proposed content matches the categories of information in Enclosure 3 of DoDI 5230.29.

Publicly accessible Website content (available to anyone without access controls) requires review and clearance from OSR *only* if the information meets the requirements of Paragraph 1, Enclosure 3, in DoDI 5230.29 because these categories include national-security and sensitive information. All information, whether national-security and sensitive information or not, must have OPSEC and PAO review, at minimum, before it is publicly released. Websites that are protected (have restricted access to authorized users only) do not have a review-and-clearance requirement from OSR.

Unofficial and special-case writing guidelines in Paragraph 6-8b, AR 360-1, include that materials requiring review must be approved / cleared before these materials are provided to – or even committed to be provided to – non-DoD publications or other public forums. Thus one reason for coordination with TRADOC PAO: to ensure all reviews for public release are conducted properly.

Some of the categories of Enclosure 3 require coordination at command level before submission to OSR. Content providers should consult the experts noted following:

- For the category “affects national security policy or foreign relations,” also consult the TRADOC G-2’s FD officer, or MSO FD officer if the content provider is assigned to an MSO or lower level.
- For the category “contains technical data, including data developed under contract or independently developed and controlled by the ITAR, that may be militarily critical and subject to limited distribution, but on which a distribution determination has not been made,” also consult TRADOC G-2’s or the MSO’s FD officer.
- For the category “new weapons or weapons systems, or significant modifications or improvements to existing weapons or weapons systems, equipment or techniques,” consult the FD officer.
- For the category “military operations, significant exercises, and operations security,” consult the organization’s or TRADOC’s OPSEC officer.

⁶⁶⁶ DoDI 5230.29; ALDODACT message 11/06.

⁶⁶⁷ Paragraph 2.4.d, Enclosure 2, DoDI 5230.29.

- For the categories of C4I and IO, consult G-6. Consult organizational security managers for COMPUSEC impact.

Appendix L

Templates for required content

Each template is recommended as a separate Webpage unless otherwise noted. Template content is set in a **different typeface**, with headers set in a **different color** than the color scheme of this *Guide*, to contrast with the narrative of the *Guide*.

TEMPLATE FOR TEXT, REQUIRED WEBSITE PURPOSE STATEMENT AND PLAN

See the “strategic Webbing” section in Chapter 4 (Page 140) for an explanation of the requirements.

We recommend pursuing the following four steps for developing the organization’s Website purpose and plan:

1. Write a general-purpose statement of what your organization wants to accomplish on its site. Since the Website must support the organization’s mission, also articulate the essential nature of the organization, its values, and its work.
2. Set goals to fulfill the purpose statement.
3. Formulate a plan to carry out the goals. Planning involves identifying the content (both text and visual theme, or design, plus navigation method and style) and interactive technologies (such as on-line forms) that your organization wants its Website to feature.
4. Get approval from your organization’s parent command / organization. You may consult your Website coordinator at any time, but you must receive Public Affairs (and OPSEC) review and approval to post the information.

Website Purpose and Plan

Website purpose / mission

TRADOC’s Website has a twofold mission: to communicate with both internal and external audiences. The Website informs its visitors of the TRADOC commanding general’s goals, priorities and intent, as keeping his command informed is one of the commander’s responsibilities. Additionally, since TRADOC’s Website is “owned” by the public, not the command, we strive to help the public understand how TRADOC supports the Army and nation in this era of persistent conflict. TRADOC accomplishes much foundational work on behalf of the Army – our aim is to make this clear to the public and to make our information relevant (the right information to the right person at the right time). The public is our “customer” and the ones who create for our organization its purpose and focus, therefore public support of TRADOC is important to us.

Our vision of enhancing the command climate within TRADOC means we will establish and sustain a long-term practice of open communication, posting materials such as fact sheets, background papers, whitepapers on key issues, or graphics/charts to aid comprehension. We will also provide a variety of information products such as news stories, posters, brochures, Web specials, and feature videos to keep our audiences informed.

Website registration

In compliance with Army regulation, TRADOC’s Website is registered and listed on the Army A-Z index, www.army.mil.

Webmaster/portal administrator contact information

If you have any questions or comments about the information presented here, please forward them to monr.webmaster@us.army.mil or monr-tradocpao@conus.army.mil.

Procedures for posting and reviewing information

All content, including links, appearing on the tradoc.army.mil domain is evaluated for fairness and acceptability as being in the best interest of the public. Tradoc.army.mil’s content will **not** exhibit hate, bias or discrimination. Furthermore, tradoc.army.mil’s content will **not** contain misleading information or unsubstantiated claims, or be in conflict with TRADOC mission or policies.

All content goes through a review process prior to posting to ensure compliance with DoD Web policy, AR 25-1, AR 25-2, AR 530-1, AR 360-1 and other applicable DoD, Army and TRADOC policy and guidance regarding Web content. TRADOC PAO serves as overall Web-content manager.

Contingency and continuity of operations



In the event of a contingency (i.e., adverse weather, pandemic influenza or terrorism attack), TRADOC's Website (tradoc.army.mil) will remain available to ensure continuous support – or, depending on conditions, will be re-established as soon as humanly and technologically possible. The Website will assist in promoting crisis programs, awareness training and other initiatives relative to the particular crisis situation, both before and after the contingency. The TRADOC Website will also assist in efforts to respond appropriately, mitigate the effects and sustain the ability of the command to accomplish its mission in the event of a threat or incident. In the event of an adverse weather contingency, the Website will be re-established and run, along with the command's headquarters, from another location. The Website content will then focus on TRADOC's internal audience (Soldiers, family members, civilian employees and the contractor workforce) since their awareness, understanding, and execution of crisis-situation measures are essential. Information and services provided to the public will be limited to the status of TRADOC facilities and their accessibility to the public.

TEMPLATE FOR TEXT, REQUIRED STATEMENT OF ORGANIZATION'S MISSION AND OUTLINE OF ITS STRUCTURE

See the "required content" section in Chapter 4 (Page 172) for an explanation of the requirements. TRADOC PAO's recommendation is to include this information on the "About Us" page so as to not duplicate content. (In fact, the content of the "About TRADOC" page follows since the command's mission and outline of its structure is integral to explaining "about us" and we do not separate the mission / structure information from the other requirements of the "About TRADOC" page.) A visual device such as an organizational chart would be helpful to Website users to depict the organization's structure.

About TRADOC

Command leadership

		
Gen. Martin E. Dempsey	Lt. Gen. David P. Valcourt	Command Sgt. Maj. David M. Bruner
Commanding general	Deputy commanding general / chief of staff	Command sergeant major
Biography	Biography	Biography
CG's Webpage		

Command's mission

TRADOC develops the Army's Soldier and civilian leaders and designs, develops and integrates capabilities, concepts and doctrine to build a campaign-capable expeditionary Army in support of Joint warfighting commanders through Army Force Generation (ARFORGEN).

Commanding general's vision

Victory starts here! TRADOC is providing the right people with the right skills, right capabilities, at the right time and right place for today and tomorrow.

To shape both today's Army and the future combat force, TRADOC:

- **Trains Soldiers**, the centerpiece of the Army: TRADOC builds the Army on a solid foundation of quality people by transforming recruits into Soldiers – Soldiers who are physically tough, mentally adaptive and live the Warrior Ethos. Soldiers are our ultimate asymmetric advantage and cannot be matched by our adversaries, current or future.
- **Develops adaptive leaders**: TRADOC trains leaders for certainty and educates them for uncertainty. Leader development produces innovative, flexible, culturally astute professionals expert in the art and science of the profession of arms and able to quickly adapt to the wide-ranging conditions of full-spectrum operations.
- **Designs today's Army modular force and the future combat force**: TRADOC identifies and integrates comprehensive solutions for the Army modular force, both today and tomorrow.
- **Maximizes institutional learning and adaptation**: As an integral component of an innovative generating force, TRADOC shapes and links it seamlessly to the operating force to maximize Army learning and adaptation.

TRADOC priorities

- Leader development (initial military training, professional military education, experience)
- Support ARFORGEN
- Future capabilities

All priorities enabled by institutional adaptation and strategic engagement.

TRADOC structure (scope and scale)

TRADOC operates 32 [schools](#) and centers at 16 Army installations. TRADOC schools conduct 2,700-plus courses, of which 300-plus are language courses. The command's training requirements have increased from a 520,000-plus student load in FY08 to a 560,000-plus student load in FY09.

Deputy commanding generals

DCG-Combined Arms/CAC commanding general

TRADOC's DCG-Combined Arms is dual-hatted as the commanding general of the Combined Arms Center, Fort Leavenworth, Kan.. CAC's CG serves as the TRADOC proponent for leader development; professional military education (officer, warrant officer, noncommissioned officer and civilian); battle command and command, control, communications, computers, intelligence, surveillance and reconnaissance (more commonly known as C4ISR); collective training; Army doctrine; and dissemination of observations/lessons learned.

The CAC commander is responsible for providing guidance, leadership and command supervision to the branch centers/schools to ensure that training remains safe, relevant, realistic and executed to Army standards. CAC's CG is also responsible for the Army's Combat Training Center Program.

DCG-Futures/ARCIC director/TRADOC G-9

The DCG-Futures is triple-hatted as ARCIC's director and as TRADOC's G-9. ARCIC develops and integrates into a Joint warfighting environment, from concept to capability, all aspects of the future force. This DCG and his team develop and integrate Joint and Army concepts, architectures and doctrine, organization, training, materiel, leadership, personnel and facilities (DOTMLPF) capabilities; validate science and technology priorities; and lead future-force experimentation. The DCG-Futures synchronizes and integrates Army capabilities with Joint, interagency and multinational capabilities.

DCG-IMT

The DCG-IMT is the TRADOC executive responsible for the Army's officer, warrant officer and enlisted training process through completion of IMT. The DCG-IMT is also responsible for providing IMT policy and execution guidance to TRADOC commanders and staff outside the IMT chain of command.

IMT encompasses reception-battalion operations that support IMT; basic combat training; advanced individual training; one-station unit training; Reserve Officer Training Corps; Officer Candidate School; Warrant Officer Candidate School; Basic Officer Leader Course Phases II and III; and recruiter, drill sergeant and other IMT cadre training.

As TRADOC transitions, a DCG-IMT will be appointed for the IMT enterprise. Currently, CG of Army Accessions Command, formerly a subordinate command of TRADOC and now a direct reporting unit to HQDA, serves as TRADOC's DCG-IMT.

DCG-Army Reserve

The DCG-Army Reserve assists TRADOC's CG in executing missions that require integration of Reserve Soldiers.

DCG-National Guard

The DCG-ARNG assists TRADOC's CG in DOTMLPF matters impacting the training and readiness of Army National Guard Soldiers and champions TRADOC programs and future initiatives through existing senior-level forums.

Deputy chiefs of staff

- **DCS, G-1/4** (personnel and logistics)
- **DCS, G-2** (intelligence)
- **DCS, G-3/5/7** (operations, plans and training)
([G-3/5/7 sites](#))
- **DCS, G-6** (command, control, communications and computers)
- **DCS, G-8** (resource management)
- **DCS, G-9** (concept development, experimentation and requirements determination)

Personal and special staff

- [Chaplain](#)
- [Commander's Planning Group](#)
- [Congressional Activities](#)
- [Equal Employment Opportunity](#)
- [Inspector General](#)
- [Internal Review and Audit Compliance](#)
- [Military History](#)
- [Public Affairs](#)
- [Quality Assurance Office](#)
- [Safety Office](#)
- [Secretary of the General Staff](#)
- [Staff Judge Advocate](#)
- [Surgeon](#)

Major subordinate organizations

- [Combined Arms Support Command](#), Fort Lee, Va.
- [TRADOC Analysis Center](#), Fort Leavenworth, Kan.
- [Center for Army Lessons Learned](#), Fort Leavenworth.

Schools

TRADOC operates 32 centers and schools on 16 [installations](#).

- [Adjutant General School](#), Fort Jackson, S.C.
- [Airborne School](#), Fort Benning, Ga.
- [Air Defense Artillery Center/School](#), Fort Bliss, Texas
- [Armor Center/School](#), Fort Knox, Ky.
- [Army Logistics Management College](#), Fort Lee, Va.
- [Army Management Staff College](#), Fort Belvoir, Va.

- [Army War College](#), Carlisle Barracks, Pa.
- [Aviation Center/School](#), Fort Rucker, Ala.
- [Aviation Logistics School](#), Fort Eustis, Va.
- [Chaplain School](#), Fort Jackson, S.C.
- [Chemical School](#), Maneuver Support Center, Fort Leonard Wood, Mo.
- [Command and General Staff College](#), Fort Leavenworth, Kan.
- [Drill Sergeant School](#), Fort Jackson, S.C.
- [Engineer School](#), Maneuver Support Center, Fort Leonard Wood, Mo.
- [Field Artillery Center/School](#), Fort Sill, Okla.
- [Finance School](#), Fort Jackson, S.C.
- [Infantry Center/School](#), Fort Benning, Ga.
- [Intelligence Center/School](#), Fort Huachuca, Ariz.
- [Military Police School](#), Maneuver Support Center, Fort Leonard Wood, Mo.
- [Officer Candidate School](#), Fort Benning, Ga.
- [Ordnance Mechanical Maintenance School](#), Aberdeen Proving Ground, Md.
- [Ordnance Munitions and Electronics Maintenance School](#), Redstone Arsenal, Ala.
- [Physical Fitness School](#), Fort Jackson, S.C.
- [Quartermaster Center/School](#), Fort Lee, Va.
- [Ranger School](#), Fort Benning, Ga.
- [Recruiting and Retention School](#), Fort Jackson, S.C.
- [School of Advanced Military Studies](#), Fort Leavenworth, Kan.
- [School of Information Technology](#), Signal Center, Fort Gordon, Ga.
- [Sergeants Major Academy](#), Fort Bliss, Texas
- [Signal Center/School](#), Fort Gordon, Ga.
- [Transportation Center/School](#), Fort Eustis, Va.
- [Warrant Officer Career Center](#), Fort Rucker, Ala.

Centers of excellence

TRADOC is transitioning to eight centers of excellence (CoEs) between FYs 2009 and 2011. Multi-branch CoEs will be:

- Field Artillery Center/School, Fort Sill, Okla., and Air Defense Artillery Center/School, Fort Bliss, Texas, will combine for the Fires CoE at Fort Sill;
- Armor Center/School, Fort Knox, Ky., and Infantry Center/School, Fort Benning, Ga., will combine for the Maneuver CoE at Fort Benning;
- Maneuver Support Center, Fort Leonard Wood, Mo. – which consists of the Chemical, Engineer and Military Police Schools – has completed transition to the Maneuver Support CoE, remaining at Fort Leonard Wood; and
- Ordnance School, Aberdeen Proving Ground, Md.; OMEMS, Redstone Arsenal, Ala.; Soldier Support Institute (Adjutant General and Finance Schools), Fort Jackson, S.C.; Transportation School, Fort Eustis, Va.; and Quartermaster School, Fort Lee, Va.; will combine into the Sustainment CoE at Fort Lee.

Single-branch CoEs are:

- Aviation Center School, Fort Rucker, Ala., has stood up as the Aviation CoE, remaining at Fort Rucker;
- Intelligence Center/School, Fort Huachuca, Ariz., became the Intelligence CoE at Fort Huachuca;
- Signal Center/School, Fort Gordon, Ga., became the Signal CoE at Fort Gordon; and

- The U.S. Army Training Center at Fort Jackson, S.C., became the Basic Combat Training CoE at Fort Jackson.

A CoE is defined as a designated training center based on TRADOC core functions that improves combined-arms solutions for Joint operations; fosters DOTMLPF integration; accelerates the development process; and unites all aspects of institutional training to develop Soldiers, leaders and civilians who embody Army values.

Staff and major subordinate organization relationships

The TRADOC headquarters staff analyzes, assesses, provides staff-management oversight and recommends for decision all activities affecting policy, command guidance, developmental processes and implementation / execution processes to support the command in meeting its mission. The staff facilitates the coordination and dissemination of strategic operational concepts and plans, doctrine and training to the Defense Department, Department of the Army, U.S. Joint Forces Command, “sister” services, Congress and external agencies and organizations. Also, the staff supports TRADOC subordinate organizations in executing command initiatives in recruiting, training, educating, designing, testing and evaluating the force.

TRADOC contacts

- TRADOC Webmaster, monr.webmaster@us.army.mil
- TRADOC Public Affairs, monr-tradocpao@conus.army.mil

See the [“Contact Us” page](#) for more information.

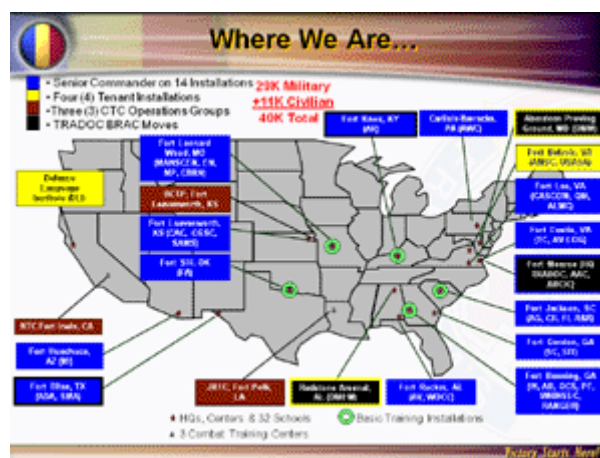
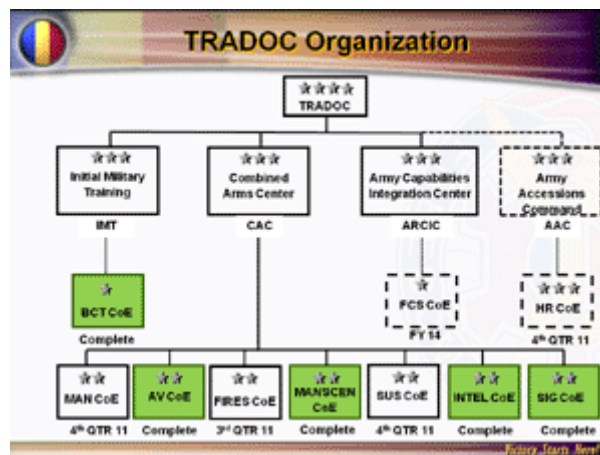
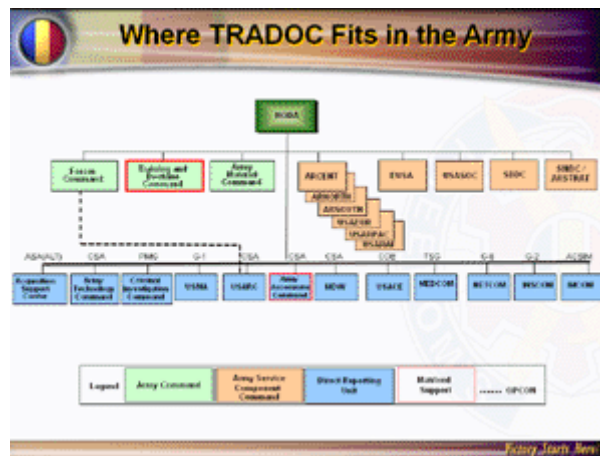
TRADOC jobs

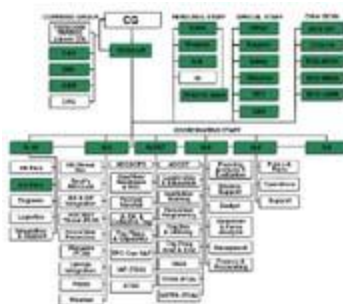
Military personnel will find TRADOC to be an assignment of choice. The TRADOC commanding general seeks combat veterans to leverage their combat experience. If interested in a job at TRADOC, check with your assignments officer.

Civilian employees will be able to contribute in building the Army’s foundation, as victory starts in TRADOC. TRADOC is supported by Fort Monroe Civilian Personnel Advisory Center, which has on-line information about anticipated vacancies at <http://www.monroe.army.mil/cpac/>. Also see the Army’s Civilian Personnel On-line at <http://acpol.army.mil/employment/index.htm>.

Organization

(all charts link to larger images)





[View organization chart](#)

TEMPLATE FOR TEXT, OTHER REQUIRED STATEMENTS

See the “required content” section in Chapter 4 (Page 172) for explanations of the requirements.

Webmaster / portal administrator contact information. We recommend that organizations include this contact information on their Website purpose plan page as well as the “Contact us” page. See Page 173.

If you have any questions or comments about the information presented here, please forward them to monr.webmaster@us.army.mil or monr-tradocpao@conus.army.mil.

Currency declaration. Army policy specifies the template for the currency declaration: “Last updated on ____” or by using a date stamp like many software programs or server functions enable. See Page 173.

This page was last updated Oct. 1, 2008

Sponsor. See Page 173.

This is an official U.S. Army Website sponsored by U.S. Army Training and Doctrine Command (TRADOC)

<title>Public Affairs homepage – sponsored by TRADOC</title>

Classification banner. See Page 173 for the text required on the first page of a Website that requires authentication / login.

TEMPLATE FOR TEXT, REQUIRED PUBLIC POLICY ON HYPERLINKS

See Page 174 for an explanation of the requirements on hyperlinks. If your organization uses external links, see the “content limitations” section in Chapter 4 (Page 170) for the requirement to publicly explain your process for linking to non-Army sites. If your organization does not use the following template, your public policy on hyperlinks, which is required to be posted to your Website, must include the following:

- Your guidelines for selecting and maintaining external links;
- Explanation of why some links are chosen and others are not;
- That the links are chosen fairly and in the best interest of the public.

Linking Policy

All hyperlinks appearing on the tradoc.army.mil domain are chosen fairly and in the best interest of the public.

Evaluation criteria

The TRADOC staff evaluates all suggested links for the tradoc.army.mil domain using the following criteria:

- Is the recommended Website an official government-owned or supported Website?
- Does the recommended Website provide official government information or services?
- Does the recommended Website complement existing information, products and services on tradoc.army.mil?
- Is the recommended Website accessible and applicable to a wide audience?

- Is the recommended Website's content relevant, useful and authoritative for Soldiers, Army civilian employees, U.S. citizens, the Army's industry partners and/or government officials?
- Does the recommended Website's information appear to be accurate and current?
- Is the recommended Website's approach to the privacy of personal information consistent with the government's privacy and security policies?
- Is the recommended Website "user-friendly"?
- Does the recommended Website meet one or more of the following "highly desirable" criteria?
 - The Website supports TRADOC's mission of training and educating the Army's Soldiers; developing leaders; supporting training in units; developing doctrine; establishing standards; and building the future Army;
 - The Website crosses military or governmental boundaries;
 - The Website enables citizens, businesses and/or government officials to conduct transactions with TRADOC, or otherwise to interact with TRADOC organizations; and/or
 - The Website provides community-level information and services, such as newcomer information to HQ TRADOC, one of its major subordinate commands, or one of its centers and schools.
- Links are reviewed and evaluated for appropriateness. If content at the hyperlink does not meet DoD/Army/TRADOC policy, the link is removed.

Links to government Websites

[Tradoc.army.mil](http://tradoc.army.mil) can add a link to any government Website that is publicly available unless directed not to by the agency that owns the site. Acceptable federal government-owned or government-sponsored Website domains include .mil, .gov and .fed.us. [Tradoc.army.mil](http://tradoc.army.mil) may also link to quasi-government agencies and Websites created by public sector/private sector partnerships; other branches of the military sites; and some government-sponsored Websites that end in .com, .org or .net until migration of these sites to .mil is complete, as required by AR 25-1.

Links to non-government Websites

In rare instances, tradoc.army.mil links to Websites that are not government-owned or government-sponsored if these Websites provide government information and/or services in a way that is not available on an official government Website. [Tradoc.army.mil](http://tradoc.army.mil) provides these non-government Websites as a public service only. TRADOC neither endorses nor guarantees in any way the organizations, services, advice or products included in these Website links. Furthermore, TRADOC neither controls nor guarantees the accuracy, relevance, timeliness or completeness of the information contained in non-government Website links. (See following disclaimer of endorsement for more information on this topic.)

Reciprocal links

We link to government information according to our linking policy, whether or not the other Website links to us. We don't engage in reciprocal linking. We invite any Website to link to tradoc.army.mil. [Tradoc.army.mil](http://tradoc.army.mil) is the official public Website for Headquarters TRADOC. Since tradoc.army.mil is a public-domain Website, you may link to us at no cost and without special permission.

Featured links

[Tradoc.army.mil](http://tradoc.army.mil) may highlight links of special interest by temporarily posting them in a position of prominence on the homepage of the Website. Featured links may be TRADOC commanding general priorities, TRADOC initiatives, seasonal information, hot topics at Army and/or DoD level, community-level services and information, and new links.

Prohibitions

[Tradoc.army.mil](http://tradoc.army.mil) will **not** link to any Website that exhibits hate, bias or discrimination. Furthermore, tradoc.army.mil reserves the right to deny or remove any link that contains misleading information or unsubstantiated claims, or is determined to be in conflict with tradoc.army.mil's mission or policies. We will not link to Websites that are not in compliance with DoD Web policy, AR 25-1 or AR 530-1.

Disclaimer of endorsement

The information posted on the tradoc.army.mil Website includes hypertext links or pointers to information created and maintained by other public and/or private organizations. Tradoc.army.mil provides these links and pointers solely for our users' information and convenience. When users select a link to an outside Website, they are leaving the tradoc.army.mil site and are subject to the policies of the owners/sponsors of the outside Website.

- TRADOC **does not** control or guarantee the accuracy, relevance, timeliness or completeness of information contained on a linked Website.
- TRADOC **does not** endorse the organizations sponsoring linked Websites, and we **do not** endorse the views they express or the products/services they offer.
- TRADOC **cannot** authorize the use of copyrighted materials contained in linked Websites. Users must request such authorization from the sponsor of the linked Website. According to the DoD Web policy, such authorization must be in writing. (See Paragraph 2.3, Part II, DoD Web policy.)
- TRADOC **is not** responsible for transmissions users receive from linked Websites.
- TRADOC **does not** guarantee that outside Websites comply with Section 508 (accessibility requirements) of the Rehabilitation Act.

Privacy and security

Please check the tradoc.army.mil "Important Notices" page for more information about TRADOC's privacy and security policies.

TEMPLATE FOR EXTERNAL-LINKS DISCLAIMER

See the "content limitations" section in Chapter 4 (Page 170) for an explanation of the requirements on external hyperlinks. The requirement for the DoD standard disclaimer for external links is given in the DoD Web policy, Paragraphs 7.1.6 and 7.1.7, Part II. The text is specified for the DoD standard disclaimer (Paragraph 7.2 of the DoD Web policy) and applies for external hyperlinks from your organization to authorized activities.

See Appendix D for the specific text of the DoD standard external-links disclaimer.

TEMPLATE FOR TEXT, REQUIRED "IMPORTANT NOTICES" PAGE

See the "required content" section in Chapter 4 (Pages 174-175) for an explanation of the requirements for this page. The "Important Notices" page describes principle policies and other important notices that govern the Website, especially those mandated by law. The privacy and security notice text from the DoD Web policy is in Appendix D; what follows is the text customized for TRADOC.

Important Notices

Privacy and security notice

This site is provided as a public service by U.S. Army Training and Doctrine Command (TRADOC). The site is intended to be used by the public for viewing and retrieving information only. Unauthorized attempts to upload or change information on this site are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1987 and the National Information Infrastructure Protection Act.

All information provided by military sources on this site is considered public information and may be distributed or copied. Use of appropriate byline/photo/image credits is requested.

We may collect information for [statistical purposes](#) [[link to breakdown of usage for statistical purposes](#)] to help us better manage this Website. That information feeds into software programs on this government computer system to create summary statistics, which we may use for such purposes as assessing what information is of most and least interest, determining technical design specifications and identifying system performance or problem areas. For site-security purposes and to ensure this service remains available to all users, we may employ software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage. Except for authorized law-enforcement investigations, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with National Archives and Records Administration (NARA) guidelines.

TRADOC's Website does not use persistent cookies, which are tokens that pass information back and forth from your machine to the server and remain after you close your browser. We may, however, use session cookies, which are tokens that remain active only until you close your browser. When you close your browser, the cookie is deleted from your computer.

Session cookies make a site easier for you to use, as they "remember" and cache information that save you time in filling out forms, for example. We don't keep a database of information obtained from these cookies. You can choose not to accept these cookies and still use the site, but you may need to enter the same information repeatedly in the form, for instance. If you choose not to accept cookies, the help information in your browser software should provide you with instruction on how to disable them.

If you have any questions or comments about the information presented here, please forward them to monr.webmaster@us.army.mil or monr-tradocpao@conus.army.mil.

How to request information under the Freedom of Information Act (FOIA)

Freedom of Information Act (FOIA) requests pertaining to TRADOC should be sent to monr.tradociapm@us.army.mil. Other FOIA requests can be made by emailing FOIA@rmda.belvoir.army.mil.

For more information on FOIA, go to

<https://www2.arims.army.mil/rmdaxml/rmda/FPHomePage.asp> or
<http://www.monroe.army.mil/Monroe/sites/installation/FOIA/foia.aspx>.

Accessibility help and information

It is the Army's policy that its Websites are accessible to handicapped users in accordance with Section 508 of the Rehabilitation Act. We review our content both before and after posting and conduct periodic audits of our Webpages/Websites to assess compliance with Section 508. However, if you find a problem with access to any of our Webpages, contact the Webmaster at monr.webmaster@us.army.mil.

Information-quality guidelines

TRADOC's goal for our on-line information is that it meets the information-quality standards of accuracy, objectivity and integrity, and to that end, the content undergoes technical, supervisory, editorial or legal review, as appropriate, based on the information's nature. Complaints about our information quality may be made to TRADOC G-6, monr.tradociapm@us.army.mil. For more information, contact the TRADOC Web-content manager at monr-tradocpao@conus.army.mil.

External-links notice

Links to non-U.S. government sites or services are solely for your convenience. The appearance of hyperlinks to non-U.S. government Websites from TRADOC's Website does not constitute endorsement by the Department of Defense, the U.S. Army and TRADOC of the linked Website or the information, products or services the site contains. For other than authorized activities such as military exchanges and Morale, Welfare and Recreation (MWR) sites, DoD/the Army/TRADOC do not exercise any editorial control over and responsibility for the information you may find at these locations. Such links are provided consistent with the stated purpose of this DoD Website.

Plug-ins

Some aspects of this site may use Apple Quicktime, Adobe Acrobat or Microsoft Word and PowerPoint. For optimal viewing [download the most recent versions here](#).

These plug-ins are provided so you can easily view documents we have on our Web. Before continuing, please read the following disclaimer for external links:

The appearance of hyperlinks does not constitute endorsement by the Department of Defense, the U.S. Army or TRADOC of the hyperlinked Website or information, products or services contained therein. For other than authorized activities such as military exchanges and Morale, Welfare and Recreation (MWR) sites, the Department of Defense does not exercise any editorial control over the information you may find at these locations. Such links are provided consistent with the stated purpose of this DoD Website.

[Adobe Acrobat Reader for .pdf files](#)
[Accessibility tools for Adobe .pdf documents](#)

[Microsoft Excel for .xls files](#)
[Microsoft Word for .doc files](#)
[Microsoft PowerPoint for .ppt files](#)
[Adobe Flash Player](#)

TEMPLATE FOR TEXT, REQUIRED “CONTACT US” PAGE

See the “required content” section in Chapter 4 (Page 175) for an explanation of this page’s requirements. As outlined in Appendix D, organizations must keep in mind that solicitation or collection of PII, including collection through capabilities which allow a user to contact the Website owner or Webmaster, may trigger the requirement for either a PA or PAS. The specific requirements for a PAS or PA are also detailed in Appendix D.

Contact Us

Write us

Address correspondence to TRADOC Public Affairs, Bldg. 27, 66 Ingalls Road, Fort Monroe, Va. 23651, or to TRADOC G-6, 84 Patch Road, Fort Monroe, Va. 23651-1051.

Call us

TRADOC Public Affairs (757) 788-3333 (DSN 680-3333)
TRADOC Webmaster (757) 788-4122 (DSN 680-4122)

Email us

TRADOC Webmaster, monr.webmaster@us.army.mil
TRADOC Public Affairs, monr-tradocpao@conus.army.mil

We do respond to email inquiries if they are appropriate inquiries. We will acknowledge that we have received your email, and what initial action we are taking with it, within two business days. Response time to resolve the issue will depend on the issue, but we pledge to give the matter the attention it warrants.

Due to the volume of emails we receive, we ask you to very carefully look at the mission information on our Website (for instance, <http://www.tradoc.army.mil/pao/index.htm> for TRADOC PAO’s mission information) to better focus your query and help us respond in an efficient, timely manner. Queries to TRADOC PAO, the proponent for information in TRADOC’s public domain, should address content (including content policy) for the TRADOC and/or TRADOC PAO Websites, or deal with other specific PAO subjects. (Due to the volume of email PAO receives, PAO cannot answer queries on non-PAO-specific topics.) Inquiries about Webpage design, navigation, network/server technical information, Website policy (other than content), and general queries involving TRADOC should be directed to the TRADOC Webmaster.

If you are a media representative with a query or request for interview, please contact the Public Communications Branch by telephone. Phone numbers are listed at http://www.tradoc.army.mil/pao/Public_Communications_Branch/index.htm.

Information-quality contact

Complaints about our information quality may be made to TRADOC G-6, monr.tradociapm@us.army.mil. For more information, contact the TRADOC Web-content manager at monr-tradocpao@conus.army.mil.

Small businesses contact

If you wish to discuss prospects for your company (if you are a small business or if you are interested in teaming with a small business), contact the Army Contracting Agency (ACA) Northeast Region small business adviser at (757) 878-3166 or (757) 873-3282.

Unsolicited proposals to the government must go through a thorough technical and contracting review. Unsolicited proposals for TRADOC should be submitted to the Northern Region Contracting Center (NRCC), TRADOC’s assigned contracting office, for contractual review – call (757) 878-4005 if you have questions regarding this process or wish to discuss contracting opportunities.

Freedom of Information Act (FOIA) contact

Freedom of Information Act (FOIA) requests pertaining to TRADOC should be sent to monr.tradociapm@us.army.mil. Other FOIA requests can be made by emailing FOIA@rmda.belvoir.army.mil.

TEMPLATE FOR TEXT, REQUIRED “ABOUT US” PAGE

See the “required content” section in Chapter 4 (Page 175) for an explanation of the requirements for this page. A previous section in this appendix, the “template for text, required statement of organization’s mission and outline of its structure” section, contains all the recommended and required “About Us” page content, as this is inseparable from the requirement to include mission / purpose and structure information.

TEMPLATE FOR TEXT, REQUIRED SITEMAP PAGE

See the “required content” section in Chapter 4 (Page 176) for an explanation of the requirements for this page. There is no template for a sitemap page, as it is unique to each location. A sitemap can be rendered either as a graphic with hotlinks or as a text listing, arranged by hierarchy and / or topic. Examples of sitemaps are TRADOC’s at <http://www.tradoc.army.mil/sitemap.htm>, or the U.S. Air Force’s, <http://www.af.mil/sitemap.asp>.

TEMPLATE FOR TEXT, REQUIRED FAQ PAGE

See the “required content” section in Chapter 4 (Page 176) for an explanation of the requirements for this page. FAQs, of course, will be unique to each organization; the following template gives a sample of possible FAQs that HQ TRADOC would receive. The U.S. Air Force’s FAQs divide into sub-topics due to the volume of questions the service receives; sample <http://www.af.mil/questions/>.

TRADOC Frequently Asked Questions

Q. How do I find publications that TRADOC publishes?

A. Depending upon the publication, you may look at the publications listing, <http://www.tradoc.army.mil/publications.htm>; access the Reimer Digital Library, <http://www.adtdl.army.mil/>, or search the Army Publishing Directorate Website, <http://www.usapa.army.mil/>. For the status of publications under revision, query the TRADOC publications officer, monr.tradociapm@us.army.mil.

Q. How do I get a job at TRADOC?

A. TRADOC jobs are listed in the projected vacancies listing hosted by the Fort Monroe Civilian Personnel Advisory Center, http://www.monroe.army.mil/cpac/anticipated_vacancies.htm, or the job announcements Webpage, <http://www.monroe.army.mil/cpac/JobAnnouncements.htm>. Current TRADOC employees possibly affected by reduction-in-force may look into the TRADOC Placement Program, http://www.monroe.army.mil/cpac/employee_placement_program.htm. Also see the Army’s Civilian Personnel On-line at <http://acpol.army.mil/employment/index.htm>.

Military personnel will also find TRADOC to be an assignment of choice. The TRADOC commanding general especially seeks combat veterans to leverage their combat experience. The TRADOC command sergeant major is partnering with the Army G-1 and Human Resources Command in a program of two-year assignments in TRADOC. If interested in a job at TRADOC, contact the TRADOC CSM’s office at (757) 788-4133.

TEMPLATE FOR TEXT, REQUIRED “HELP” PAGE

See the “required content” section in Chapter 4 (Page 176) for an explanation of the requirements for this page. The “Help” page outlines major proposed and implemented changes to the Website.

Help

The nature of the Web is change. We also strive to present our Website users with the best possible Web presence. To that end, major proposed or implemented changes to our Website will be listed here to assist our visitors in finding the information they need.

Proposed changes

A Web special on Army Career Tracker to introduce you to this tool for guided self-development for enlisted Soldiers, officers and Army civilians. ACT “guides” in the areas the Army thinks you need for your skill set and tracks where you’ve been and where you need to go.

Implemented changes

“TRADOC In-depth” video stories featuring events and trends in TRADOC.

<http://www.tradoc.army.mil/pao/videos/indepth.htm>.

For more help, see the [sitemap](#).

TEMPLATE FOR TEXT, REQUIRED SEARCH PAGE

See the “required content” section in Chapter 4 (Page 176) for an explanation of the requirements for this page.

Some Webpage software offers an automated search component as a search page, but most sites employ a search box. There is no template for the search box; the Webmaster must set it up.

Appendix M

Writing for the Web

What do you emphasize when you create Web content? There are some guidelines – some common characteristics – that Web content shares with journalism news articles:

- The basic principles for writing are the same;
- Web content should emphasize *news values* just as a newspaper article does;
- Web content should be as readable as a journalism story;
- The *inverted pyramid* style of writing serves Web content as well as it does print journalism – with some modification; and
- Web content consists of the same parts – *lead, bridge, body, ending* (or should) – as print-journalism writing and makes the same mistakes as poor journalism writing does.

This appendix gives tips for improving Web content.

THE BASIC PRINCIPLES

Web content, like a typical journalism news story, should give details that answer the six basic questions of the “five Ws and H” (*who, what, when, where, why, and how*). As outlined in Chapter 2’s “10 commandments for content providers,” tell the content reader who’s involved or who the information is for; what the content is about; if involving a timeline or event, when it is taking place; where the event is taking place; why it is taking place (ties to *relevance*); and, if applicable, how it is taking place.

Another basic principle for Web writing is to apply the ABCs of journalism:

- **Accuracy** – Get it down right;
- **Brevity** – Keep your sentences and paragraphs short;
- **Clarity** – Avoid using too many words. Don’t be repetitious. Keep related ideas together. Keep it simple.

NEWS VALUES

The more news values a piece of information has, the more “newsworthy” it is, and therefore the more interesting and attractive a potential Web visitor will find it – although we say this with a caveat, as today’s news consumers consider something to be newsworthy if it affects his / her life (a self-centric way of relating to information). The news values are:

- **Timeliness** – Information that happened recently should be posted without delay. For the Web, “recent” is near-real-time – within 12 hours, preferably, but at maximum, no greater than 24 hours. Today’s news consumer has a news diet of two or three days maximum, then moves on to another topic.
- **Immediacy or currency** – Posting information on events very soon after they happen reflects timeliness, but a “kissing cousin” of this element, immediacy, reflects that the information is of current concern to a lot of people.
- **Proximity** – Information has proximity if it happened nearby.
- **Impact**, also called **relevance** – The information directly affects your audience. TRADOC Web content needs to point out how the information is relevant to the Web visitor.
- **Suspense** – Information that has this element will keep the reader wondering what’s going to happen next.
- **Prominence** – Information has this element if it involves a person or organization that all Website visitors may be interested in.
- **Oddity** – Information has this element if it’s about something unusual or strange – something out of the ordinary. Editor Charles Dana once said, “If a dog bites a man, that’s not news. But if a man bites a dog, that’s news!”
- **Conflict** – Information has this element if it involves a disagreement between two or more people, for example, or is an opposition of some sort, such as a sporting event.
- **Emotion** – Information may excite or disturb the reader, and thus have human impact; although the content doesn’t directly affect the reader, such as with the impact / relevance element, people will avidly read it

anyway. A Soldier's 4-year-old son, for instance, is killed in a hit-and-run accident. Even though one person, the child who died – and one family – the one that must bury him – was directly affected, many readers will feel a strong emotional response to this situation.

- **Progress** – Information has this element if it details changes in the way the Army is doing things.

READABILITY

Writing well is an important task for the content provider, so this section outlines some proven principles to improve readability. To do this, use:

- **Short sentences**, an average of 15-20 or fewer words. Short sentences are easiest to understand. Vary sentence length to avoid chopiness. In longer sentences, use punctuation properly to help the reader.
- **Short paragraphs**, one main idea / concept to a paragraph. One or two sentences per paragraph is usually enough.
- **Easy words**, three syllables or fewer. If you must use a longer, harder word, such as a technical word, explain it with a simple definition or pithy analogy, then refer to it thereafter in a shortened or simplified form.
- **Personal words**. These bring in the human interest: *I, you, me, they*, plus names and quotes.
- **Active verbs**. These are words that show action, such as those found in a newspaper's sports pages. Avoid passive voice as much as possible because it's indirect, unfocused, and often hides the doer of the action. By contrast, the active voice is direct, natural, and forceful. It emphasizes the doer by putting the doer before the verb and showing who or what does the action. It makes sentences clearer and shortens sentences. (Eliminating passive voice can tighten content by about 20 percent.) The standard English sentence order of subject-verb-object is best.
- **Concise sentences**. Avoid extra words – don't use two words to express an idea where one will do. Examples: delete *in order* in the phrase *in order to*; delete *of all* in *first of all*; delete *future* from *future plans* (*plans* implies they are yet to happen).

Word choice is important, and that's what makes writing hard work. Avoid a profusion of adjectives and adverbs, and choose your nouns and verbs to **show** your reader, rather than **tell** him / her. Be specific; try to avoid abstraction; don't cite dry facts alone. If you're too vague, the reader may think you mean one thing when you mean another. Example: If you want to describe "fat," try also to have a doctor say that "fat" is 300 pounds. If you use statistics, "translate" them into terms the reader can understand, that have meaning, and / or can be visualized.

Example of what not to write: *More than 8,800 people die every year on America's highways*. Example of what to write: *About 170 people die every day on America's highways* (more understandable / more meaning than the larger number of 8,800) or *Enough people die every year on America's highways to fill Yankee Stadium* (can be visualized).

Tips to write concise sentences and eliminate passive voice:

- Watch for "Latinized suffixes" such as *tion, ment, ize, ility*. A Latinized suffix often means the word was a verb, but the suffix made the word a noun. Example: *The NCO is responsible for the motivation, development and supervision of his squad*. Rewritten, this sentence should read: *The NCO motivates, develops and supervises his squad*. The correction gives the sentence action verbs and gets rid of extra words.

A classic example of Latinized suffixes comes from George Orwell: *Objective consideration of contemporary phenomena compels the conclusion that success or failure in competitive activities exhibits no tendency to be commensurate with innate capacity, but that a considerable element of the unpredictable must inevitably be taken into account*.

Orwell, tongue-in-cheek, was rephrasing the better-known verse from the Bible's Book of Ecclesiastes: *I returned, and saw under the sun, that the race is not to the swift, nor the battle to the strong, neither yet bread to the wise, nor yet riches to men of understanding, nor yet favor to men of skill; but time and chance happens to them all*.

- To recognize (and get rid of) the passive voice, look for one of the eight forms of "to be" verbs (*am, is, are, was, were, be, being, been*) or a verb ending in *en* or *ed*. Examples: *is requested, were eaten, was completed*. To fix the sentence construction, put the doer of the sentence as the subject. For example,

rather than write *The PT test was passed by Jones* (passive), write *Jones passed the PT test* (active voice; the doer, Jones, is before the verb).

THE INVERTED PYRAMID

Closely aligned with making a story readable is getting to the point fast. Readers don't have time to wade through a bunch of words before finding out what the content is all about, so we recommend that you write in an inverted-pyramid style. By writing in this style, you allow your reader to get the meat of what you want to tell him / her, even if he / she reads it only partway through.

The inverted pyramid was adopted because editors cut stories from the end to make them fit into a newspaper's available space, but busy Web visitors like the inverted-pyramid style because they only have to read the headline and first paragraph or two to get the jist of the content. "Inverted pyramid" is a metaphor for the broad base of the important facts first, in the first paragraph or two; with details following in descending order of importance; ending with the least important but still-relevant information.

The inverted-pyramid style, with some practice, should come naturally to you. After all, it's actually the way you tell friends about something important in your life. Or: how do children tell a story? You ... children ... most human beings ... have this in common: normally you blurt out the important facts fast, using plenty of action verbs.

Inverted-pyramid writing is the same concept. You start with a *lead* (pronounced LEED), which summarizes the content's most important information and contains specific facts answering most, if not all, of the five Ws (and possibly the H). This kind of lead is called a *summary lead*, not surprisingly, and its function is twofold: to not only state important facts first, as mentioned, but to also attract the casual Website visitor into being a reader of your content.

You follow the lead by developing more details from a piece of information introduced in the lead. (Don't begin here with a chronological narrative.) Your third paragraph (and consecutive paragraphs) expands even more on these details.

You choose what goes in the lead, what follows the lead and, indeed, what even is included in your content by selecting facts based on their news value, already mentioned. Fortunately, the important facts ordinarily are the Ws and H, so you select which of the Ws and H is most important, and that ordinarily will be what attracts the Website visitor.

For example, the most important fact (which should come first in the first sentence) is not always to name a person (*who*). Some content should emphasize the time element (*when*) if it plays the most important part. Or, if your content's setting (*where*) is unusual or important, play that up. When a thing or action is noteworthy (*what*) and overshadows other facts, it should be featured at the beginning.

You may not know the *why* or *how*, but if you do, it may not be necessary to answer these questions in the lead sentence. (Second or third sentence may do.) However, there will be times when a person's motive, cause, or reason (*why*) may be compelling and should come first. (And you should definitely answer the question of *why* it's relevant to the Website visitor in the first screen – see Chapter 2). Or, the circumstances or way something is accomplished (*how*) may be most important.

Before posting the information comes the modification: you determine how your information will be arranged in Webpages and blocks of information. The Website's first release of information should stay with bare facts (the *who*, *what*, *when*, and *where*) and should be a short, timely burst of information, much like a tweet on Twitter. Within a short cycle (remember, the maximum length of interest in a news topic averages two or three days), update the facts to convey timeliness and relevance. Provide links to the back story (background information and / or the *why* or *how*) and future stories / more in-depth feature spin-offs. In other words, you break up the material into short pieces, enrich it with links to back stories / spin-off stories, and you update it in cycles that amount to hours, not days. Content is arranged in "blocks" that lend themselves to division among Webpages – and there should be definite "meat" in the background-story and feature-reporting aspects. As an Associated Press study (<http://www.ap.org/newmodel.pdf>) found, its subjects were "overloaded with facts and updates and were having trouble moving more deeply into the background and resolution of news stories." Since most news consumers crave a chance to find out the back story, providing it will draw traffic to your Web content.

CONTENT'S NATURAL PARTS

We've mentioned that Web content, like a news story, has a *lead*. Web content, and most straightforward writing, also consists naturally of a *bridge*, *body*, and *ending*. Each division should accomplish certain things.

Your content's first five to 10 words ... first sentence ... first paragraph ... "hook" the reader in, establish your subject, set your content's tone, and guide your reader into the rest of your content. The lead should captivate readers in the first line or two, letting them know why they should take the time to read your content. A Web-content provider's greatest efforts and ingenuity are needed to capture the Website visitor's attention in the content's lead.

A lead should be short – usually one sentence of no more than 25 words as a rule of thumb – and should capsule the content by covering most of the five Ws and H, as mentioned.

The bridge is usually a one-, two- or three-sentence paragraph between the content's lead and its main body. The bridge eases the reader into the body, linking the lead to the body; backs up or adds information to the lead; and answers any of the Ws and H not covered in the lead.

Elaborating details beyond the bridge make up most of the rest of the content, called the body. The body expands the material covered in the lead and bridge. The body should develop the content and continue the lead's mood or tone. The body should have a single focus and not sidetrack into other topics. (Supporting information that will help your reader understand your topic better can be placed in a "sidebar" linked from the main content.)

Just as a journalism news article written in inverted-pyramid style doesn't have an ending, per se – it ends when all pertinent facts have been included – most Web content will end in the same manner. However, if your Web content asks the reader to do something or to avoid something, there should be a clear "call to action" – specifics on what to do or avoid – in the content's conclusion.

If you ask your reader to do something / not do something, that's *opinion content*. Opinion content should not contradict or criticize DoD, DA, or TRADOC policy; hold the Army or any of its members up to ridicule; take sides in political issues; hold any race, religion or ethnic group up to ridicule; violate host-country sensitivities; or be written to air personal complaints.

Each paragraph from lead to bridge to body to ending should have a logical connection to the preceding one. The second paragraph, for instance, may be linked to the lead by a repeated name. A quote as the third paragraph naturally follows a quote paraphrased in the lead or bridge. In the fourth paragraph, content introduced by the word "Another" ties back to information already brought up. These word links are called *transitions*, and they're necessary to keep your content's flow smooth and logical. Especially concentrate on using transitions throughout the body – from paragraph to paragraph, section to section – to maintain flow.

COMMON MISTAKES

There are seven common mistakes to avoid when writing your lead sentence:

- **Periodicity.** A periodic sentence is one that doesn't yield its meaning until its end. As a lead, such a sentence slows the reader, and perhaps confuses him because it throws too many facts his way and will lose his interest.

Don't write: *Increases in the cost of cloth and buttons to the Army, and the necessary flow-through of these costs to Soldiers, are the reasons the Army is radically decreasing Soldiers' monthly clothing allowance.*

This sentence is more than twice as long as the recommended average and uses an abstract adjective (radically), but its worst error is that the reader must go to the sentence's end before he gets to the important point (the smaller monthly clothing allowance).

- **Date first.** The date usually is the least important of the five Ws and H, even in Web content that reports events or information that day.

Don't write: *On April 16, 552nd Training Battalion's tax adviser office, located at 1552 TRADOC Road, will close.*

Preferred: *The 552nd Training Battalion's tax adviser's office will close April 16.* Then comes the next paragraph with elaborating details: *The office, located at 1552 TRADOC Road, ...*

- **Person's name first.** What a person is announcing is usually more important than the person making the announcement, even if that person is the commander, and therefore the *what* of the announcement comes first, with the announcer's identity (*who*) of secondary importance. Instead of: *Lt. Col. Gordon Jackson, 552nd Training Battalion's commander, announced April 9 that Good Friday would be a battalion training holiday and "to hell with those who holler about separation of church and state."* Write: *Good Friday is a battalion training holiday and "to hell with those who holler about separation of church and state," Lt. Col. Gordon Jackson, 552nd Training Battalion's commander, declared April 9.*
- **"There" or "The."** It may be difficult to avoid beginning a sentence with either of these words, but if a writer begins in this way, he / she will probably write in the passive voice. Remember the example, "The PT test was passed by Jones"?
- **Cutesy / clever but nothing to do with the content.** You may think it's snappy and it may attract the reader, but it will eventually irritate him / her as well. The reader wants to get to the meat of the content as soon as possible and will resent being tricked. You also have the danger of cutesy being degrading.

An example of cutesy / clever: *Sugar and spice and everything nice. That's what little girls are made of. But what about big girls?* The actual story had nothing to do with sugar, spice, or little girls – it detailed the challenges of a female military police officer in an all-male environment.

Would you like this type of lead? No? Then don't write it for others to read.

- **"So" statement.** There's no possible disagreement with these beginnings and evoke a "So?" response from the reader. Example: *Retirement means many things to different people.* What does retirement mean to the person being portrayed in this content? That's the lead.
- **Jamming everything into the first sentence.** You may not even get everything into the first paragraph – those are the elaborating details to be contained in the content's bridge and body.

Here's an example of a sentence that tries to contain too much: *The 2009 noncommissioned officer evaluation survey is now underway, and promotions are being delayed while an Army-convened panel analyzes the recent glut of every NCO being rated "top block" as well as clarity of regulations and guidelines governing NCOERs.*

Appendix N

Section 508 compliance standards

As stated in Chapter 4, the foundational document for Section 508 compliance standards is Subsection 1194.22 of the federal law, Section 508 of the Rehabilitation Act. For more information on the W3C's accessibility guidelines, which the law's accessibility criteria were based on, see the Web Accessibility Initiative (WAI) team's Website, www.w3c.org/wai/, and the Priority 1 checkpoints in WCAG 2.0, <http://www.w3.org/TR/WCAG/>. Also see the Section 508 Website, <http://www.section508.gov>.

To make Websites Section 508 compliant, follow these accessibility standards:⁶⁶⁸

- A text equivalent must be provided for every non-text element, such as "alt" (alternative text attribute) or "longdesc" (long description tag), or in element context. Alternate text tags must convey useful descriptions of the graphic to allow interpretation by users with visual-acuity problems – do not use "photograph" as the text tag when posting a picture of basic training or equipment, for example.
- Information conveyed with color must also be available without color – for example, from context or markup. Colors may not be used alone to depict degrees of importance or emphasis.
- Section 508 compliance requires that Webpages be designed to avoid causing the screen to flicker with a frequency greater than two hertz (Hz) and lower than 55 Hz. However, Webpages should not use blinking, flashing, flickering, or scrolling text, graphic, or marquee elements, nor flying text or continuously animated graphic-image format images (restrict the repetition of animations to one or two cycles rather than continuously looping).
- Documents must be organized so they are readable without requiring an associated style sheet.
- Webpages that function as equivalents to dynamic content must be updated whenever dynamic content changes. The content of a text-only page, for example, provided to make a Website comply with the requirement to have equivalent information and functionality must be updated whenever the primary page changes. Equivalent pages should be provided only when compliance cannot be accomplished any other way.
- Use redundant text links instead of server-side imagemaps except where the regions cannot be defined with an available geometric shape.
- Use client-side imagemaps whenever possible in place of server-side imagemaps.
- Data tables must have row and column headers identified.
- Use markup and style sheets properly to assist navigation. Use markup to associate data cells and header cells for data tables that have two or more logical levels of row or column headers.
- Use of frames is not encouraged. However, if used, frames must be titled with text that facilitates frame identification and navigation.
- When an alternative accessible Webpage uses a plug-in, applet, or other application, and a link to that plug-in, applet, or application is provided, the plug-in, applet, or other application must be present on the client system to interpret page content.
- Provide a method that permits users to skip repetitive navigation links.
- When pages use scripting languages to display content or to create interface elements, script-provided information identified with functional text must be provided that can be read by assistive technology.
- When electronic forms are meant to be completed on-line, a form must also be offered to allow people using assistive technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.
- When a timed response is required, the user will be alerted and given enough time to indicate more time is required.

Also, Army public Websites must, to the maximum extent feasible, minimize page-download times for their visitors.⁶⁶⁹

⁶⁶⁸ Paragraph 8-7b(17), DA PAM 25-1-1. Also see Paragraph 1194.22 of Section 508.

⁶⁶⁹ Paragraph 8-3b(1), DA PAM 25-1-1.

Navigational aids will place visitor usability over “cool design” considerations:

- Graphic navigational aids, such as buttons or icons, should be provided to allow easy navigation by visually impaired users. ALT text must be used for graphics. However, the incorrect way to write an ALT tag is as “red arrow pointing left” or something similar; the correct way is to describe the Webpage the graphic is linked to, such as “link to background information on the Instructor of the Year competition.”
- Pop-up and drop-down menus should not be used without providing alternate non-active means of navigation such as sitemaps or imagemaps. Pop-up and drop-down menus pose great difficulty to persons with manual-dexterity disabilities – some of whom may make up part of the target audience as employees who suffer from carpal-tunnel syndrome, for example.

DoD’s 13 “rules” were issued before DA PAM 25-1-1 formalized the standards more, but they are still good guidelines. Although there is some redundancy with the standards in DA PAM 25-1-1, we have updated them to include WCAG 2.0 guidelines:

1. **Provide text alternatives for all non-text content.** Ensure “ALT” text is on all graphics, including bullets, for instance. Text alternatives enable people to change non-text forms into other forms they need, such as Braille or symbols. Non-text content includes images, graphical representations of text (including symbols), imagemap regions, animated GIFs, applets and programmatic objects, ASCII art, frames, scripts, images used as list bullets, spacers, graphical buttons, sounds, stand-alone audio files, audio tracks of video, and video. Provide alternatives for time-based media.
2. **Meaning must be independent of color.** Color may not be used as the only visual means of conveying information, indicating an action, prompting a response, or distinguishing a visual element. Make it easier for users to see and hear content, including separating foreground from background via color contrast.
3. **Identify language changes.** Applies if a foreign language used in the Website; identify the language in the HTML code. Also, the W3C requires that the default human language of each Webpage be programmatically determined, as well as the language of each passage or phrase in the content. The exceptions are proper names, technical terms, words of indeterminate language, and words or phrases that have become part of the vernacular of the immediately surrounding text. As part of the W3C’s overarching concept that text content be readable and understandable, the W3C also recommends that a mechanism be available for identifying: 1) specific definitions of words or phrases used in an unusual or restricted way, including idioms and jargon; 2) the expanded form or meaning of abbreviations; and 3) the specific pronunciations of words where meaning of the words, in context, is ambiguous without knowing the pronunciation. The W3C also requires that when the text is difficult enough that it requires a reading ability more advanced than the lower secondary-education level (after removal of proper names and titles), include supplemental content or a version that does not require a reading ability more advanced than the lower secondary-education level.
4. **Content must be stylesheet independent.** When an HTML document is rendered without associated stylesheets, it must still be possible to read the Webpage.
5. **Update equivalents for dynamic content.** Static (text only, most often) pages used as alternates must be updated as often as “dynamic content” pages. Provide straight text hyperlinks for JavaScript drop-down menus and flowing menus. Follow the concept of “equivalent facilitation” – one of Section 508 law’s most important concepts – which requires the same access on your Website for the disabled as for non-impaired people.
6. **Include redundant text links for server-side imagemaps.**
7. **Use client-side imagemaps whenever possible.** Most imagemaps are client-side imagemaps. Include “ALT” text for their hotspots IAW Principle 1.
8. **Identify row and column headers in data tables.** For data tables that have two or more logical levels of row or column headers, use HTML markup to associate data cells and header cells. Webpages must appear and operate in predictable ways. For instance, when any component receives focus, it does not initiate a change of context. Or, changing the setting of any user-interface component does not automatically cause a change of context unless the user has been advised of the behavior before using the component.
9. **Data cells must be associated with header cells.** Tables for layout are OK – top screenreaders will read them. However, create content that can be presented in different ways (for example, simpler layout than a table) without losing information or structure. When the sequence in which content is presented affects its

meaning (such as a data cell), a correct reading sequence must be able to be programmatically determined. Instructions for understanding and operating content must not rely solely on sensory characteristics of components such as shape, size, visual location, orientation, or sound.

10. **Title all frames.** Set target properties to avoid nesting frames. Title each frame to facilitate frame identification and navigation. Also, navigational mechanisms, such as frames, that are repeated on multiple Webpages within a Website must occur in the same relative order each time they are repeated, unless a change is initiated by the user. Components that have the same functionality within a Website, such as frames, must be identified consistently, such as titled.
11. **Each Website must be script independent.** Like Principle 4, ensure pages are usable when scripts, applets or other programmatic objects are turned off or not supported. Do not make your navigation rely completely on a JavaScript function! Provide equivalent links in the form of text hyperlinks. Content must be robust enough that it can be interpreted reliably by a wide variety of user agents, including assistive technologies. Further, ensure markup-language elements have complete start and end tags, elements are nested according to their specifications, elements do not contain duplicate attributes, and any IDs are unique. Ensure that the name and role of all user-interface components (including, but not limited to, form elements, links, and components generated by scripts) can be programmatically determined; that the user can programmatically set states, properties, and values; and that notification of changes to these items is available to user agents, including assistive technologies.
12. **Synchronize multimedia equivalents.** Provide an auditory description of important information on the visual track of any multimedia presentation. For any time-based multimedia presentation (movie or animation), synchronize equivalent alternatives (captions or auditory descriptions of the visual track) with the presentation.
13. **Provide the option to skip repetitive links.** Make sure the Web user, whether non-impaired or impaired, can use the tab key to tab through your Webpage (associate labels with form methods, for instance). Use anchors/bookmarks to jump over repetitive sections of pages.

Some other helpful recommendations (for a complete list, see the WCAG Webpage) include:

- Provide users enough time to read and use content. For instance, if your Website has a time limit on any content, enable the user to turn off, adjust the time limit, or extend the time limit.
- Enable users to pause, stop, or hide moving, blinking, scrolling, or auto-updating information. The user should also be able to postpone or suppress interruptions except those involving an emergency, as well as continue activity without loss of data after re-authenticating when an authenticated session expires. Very important: do not design content in a way that is known to cause seizures; Webpages must not contain anything that flashes more than three times in any one-second period, or the flash is below the general-flash or red-flash thresholds.
- Provide ways to help users navigate, find content, and determine where they are on your Website. For instance, provide a mechanism to bypass blocks of content that are repeated on multiple Webpages. Webpages must have titles, headings, and labels that describe their topic or purpose. Use section headings to organize content. The user should be able to determine each link's purpose from the link text alone or from the link text together with its programmatically determined link context. The W3C also encourages "breadcrumb" navigation so that more than one way is available to locate a Webpage within a set of Webpages and that information about the user's location within a set of Webpages is readily available.
- Help users avoid and correct mistakes. Provide labels or instructions when content requires user input. If an input error is automatically detected, the incorrect item should be identified and the error described to the user in text. For Webpages that require the user to submit information (especially legal, financial, or personal data), submissions should be reversible, check-able, and confirm-able. For "check-able," data entered by the user is checked for input errors and the user is provided an opportunity to correct them. A mechanism should also be available for reviewing, confirming, and correcting information before the user finalizes the submission. Lastly, context-sensitive help should be available to the user.

Appendix O

Measuring the success of your publicly accessible Website and social-media engagements

In the “strategic Webbing” section of Chapter 4, we discussed the importance of knowing what our Website visitors want from us. This can only be discovered through measurement and analysis.

Social media has changed the paradigm for publicly accessible Websites. Website visitors expect a potential for collaboration, or at least interaction, and if there isn’t some evidence that there’s two-way communication, they go elsewhere. Communication on the Internet these days is collaborative, egalitarian, and democratic. Anyone may speak and be heard, as opposed to traditional media (print, radio, television) and even Websites of a few years ago, where there were only a few voices and “party line” messaging.

Even if this phenomenon of social media hadn’t occurred, Army Web-content managers must analyze how well they’re doing in providing the American public the information they need to be good citizens. Many Army Websites do this well; others would find an assessment eye-opening as to how bad they are.

So what *do* Website visitors expect of Army Websites? Simply put: conversations, social networking, content-sharing, accessibility of information, honesty / ethics, and transparency. Same as they expect from the dot-com Internet. Conversations like they enjoy in Blogger, Twitter, message boards, and even via on-line forms for feedback. Social networking like they’re used to in Facebook, LinkedIn, MySpace, and niche networks. Content-sharing like they get in YouTube, Flickr, Delicious and podcasts. Searchability / accessibility like they rely on with top search engines Google, Bing, or Yahoo, for example. They expect participation – that our messaging has a human presence behind it and that blogs sound like a real person. They are no respecters of rank or optempo – they expect us to try and build communities, not treat them as audiences to be talked at. They expect us to be frank and open with them.

Employing publicly accessible Websites, especially social-media sites, enables leaders and Army professional communicators to build communities by allowing members of the public to ask questions and design their own experience with the Army.

The problem is knowing how successful you are in this. That’s why this appendix offers some best practices and samples. However, no DoD entity we could find measures / analyzes their Website and makes those results available on the public Internet, so there’s not much material for comparison. As we gain lessons-learned, we expect our best practices, even our measurement and analysis instruments, to transition quickly during the next few months.

BEST PRACTICES AND LESSONS-LEARNED

How can organizations evaluate their effectiveness on the Web? This section is our lessons-learned on the subject. Also see the “strategic Webbing” section in Chapter 4.

First, let’s talk about what not to rely on. Don’t use hit counters; they aren’t a good measurement. As measurement and analysis guru Katie

Feedback reporting: the mysterious requirement

Policy, in a nutshell, says to measure and analyze, but doesn’t say how. The concept in DoD Web policy and throughout AR 360-1 is that Websites / Web-based applications would be measured via feedback. Following are the places in DoD and Army policy that state or imply the requirement for feedback or self-assessment.

From DoD Web policy, Part II:

Paragraph 3.1: DoD component heads and heads of subordinate organizations that establish Websites are responsible for instituting a process. ... The steps of this process include:

3.1.9. Feedback reporting, to include “lessons learned.”

4.1. Procedures ... must be established and, as a minimum, address the following:

4.1.14. Incorporating a feedback mechanism for users’ comments in accordance with the [PRA] of 1995.

(*Caveat:* per Paragraph 11.1.2, Part II, the PRA applies to electronic forms / information collections on Websites that collect standardized information from the public. It does not apply to collection of information strictly from current DoD employees or service members in the scope of their employment. Surveys on publicly accessible Websites will not ordinarily be exempt from the requirement to obtain OMB approval under this exception.)

4.2. Verification. Procedures must be established for each DoD Website to ensure that:

Delahaye Paine says, “hits” equals “how idiots track success.” One reason for the disdain is that hit-counter numbers are suspect because counters may not start at zero – a site’s Webmaster can set his / her own starting number and reset it as he / she pleases. Also, since hits correspond to “visits,” refreshing the Web browser counts as a hit. The third reason to suspect counters’ reliability is because a graphic on a Webpage generates a *request* on the Webserver. Each graphic is a separate request. Therefore a page with seven graphics on it will count eight hits – one for each graphic and one for the HTML page visit. A page with four graphics on it counts five hits for each visit. The page with seven graphics may be only as popular as, or less so, than the one with four graphics, but the hit counter on the page with seven graphics will count many more hits than on the page with four graphics.

To measure, you must **first precisely define the parameters of success.** Measuring success is more than just numerical – it’s in the email you get; it’s in how navigable your site is and how many headaches you give your visitors; it’s in how well your site is designed; it’s definitely in how well you back up good design with good content. The key to a successful Website is user-centered design, as we stated above. A successful Website is useful to the user, usefulness being a combination of utility and usability. Utility is the site’s functionality and ability to meet the visitor’s needs. Usability is the user’s ability to manipulate the site’s features to accomplish a particular goal. Usable sites are efficient, easy to learn, and help users accomplish goals in a satisfactory and error-free manner.

So, yes, **you can crunch numbers to measure success, although you won’t completely capture success via numbers.** There are a number of automated tools on the Internet – free and not free – that specialize in Web analytics. You can gather input from the grader.com family of tools on your social-media sites: facebook.grader.com, blog.grader.com, and twitter.grader.com, all free. Be sure to compare your Website with competitors’ at Website.grader.com. The grader.com tools and xinureturns.com (also free) are best consulted for search-engine optimization and page rankings.

Some form of Web analytics is necessary to even begin to quantify and measure success – Woopra.com is recommended if you can’t use Google Analytics (free). Woopra is also free but requires download of a widget. Both ComScore, comscore.com, and Nielsen NetRatings, nielsen-netratings.com, measure Web traffic such as page views, hits, and visits; neither are free. More traffic stats can be obtained via sites like ClickTracks, clicktracks.com; Compete, compete.com; WebTrends, webtrends.com; and Omniture, omniture.com, for example. ClickTracks, WebTrends, Omniture, and most of Compete’s most useful stats aren’t free, but the thing to know here is that you are not forced to rely on your DOIM’s release of server logs to quantify Web traffic – there are other options.

Other free sources of stats include Google News, Google Blog Search, Really Simple Syndication (RSS) feeds, and Twitter Search. How active someone is in social media may be determined via twinfluence.com. To see the last 20 places someone went, check tealium.com (not free).

Some sites specialize in blog rankings: Technorati, technorati.com; Ice Rocket, icerocket.com; BlogLines, bloglines.com; and Kineda, kineda.com/are-you-an-a-list-blogebrity and kineda.com/?p=1166 (widget), for example. Blog rankings are measured by the number of links to them, trackbacks, and comments, according to Paine. Two other sites

4.2.1. A comprehensive, multi-disciplinary security assessment addressing both content and technical issues is conducted at least annually.

4.3. Feedback reporting.

4.3.2. Website content providers and administrators will support and participate in the feedback reporting system.

4.3.3. Website content providers and administrators will review “lessons learned” and incorporate content and security changes where appropriate.

From AR 360-1:

Paragraph 2-4g: Advise the commander on audience attitudes about and perceptions of policies, programs, and information needs. Such advice may come from informal surveys. ...

Paragraph 5-6c(5): Public affairs officers will assess and evaluate all audiences to develop a sound PA program.

Paragraph 8-1d(4): The CR council, managed by PAO, evaluates the possible effects of command operations and policies on community relations, and advises the commander of actions that can reduce or prevent adverse reaction. Paragraph 8-1d(7): The CR council conducts a periodic appraisal of public attitudes toward the command. ...

Paragraph 8-1e: Community surveys and analyses are helpful in developing a sound community relations program. Army FM 46-1-1 has guidance on conducting community surveys. Caution will be taken to ensure that surveys do not violate the FOIA, the Privacy Act, or AR 380-13, which concerns the acquisition and storage of information on non-affiliated persons and organizations. (IAW AR 380-13, Paragraph 2a, Army policy

measure blogs via the number of links to them: Feedster, feedster.com; and BlogPulse, blogpulse.com. However, most blogs on the dot-mil aren't popular enough to register on the blog-ranking sites' charts. Of more use may be Biz360, biz360.com, which has a metric (not free) called Media Signal that looks at positive, negative, and neutral coverage in blogs and then factors in links and connections with an index number to gauge a blog's total impact.

If you want to conduct a user survey, both SurveyMonkey, surveymonkey.com, and Zoomerang, zoomerang.com, offer basic survey-building free. Surveys can be administered on-line. SurveyMonkey's "basic" service is limited to 100 responses per survey, so if you're conducting a survey where you expect more than 100 responses, you'd need to upgrade to their "professional subscriber" service (not free). SurveyMonkey's question choices also do not offer radio-button selection (best method for yes / no or either / or responses) and thus may alter the way you phrase your survey questions. Zoomerang can import a survey you've already built in Survey Monkey, or you can create a survey from scratch within Zoomerang. Zoomerang, which also has a free "basic" service, offers a useful customer-satisfaction-survey template but limits surveys to 30 questions per page – if you're judicious about how you set up your answer scale, you can combine questions in a matrix.

On-line survey tools like SurveyMonkey and Zoomerang will help you analyze your Website visitors' perceptions of your content to find your strengths and weaknesses. A pattern of "2" answers on a scale of one to five where one equals poor; two equals fair; three equals good; four equals very good; and five equals excellent, for instance, will give you strong indicators that certain areas of your site need improvement.

But what do you do with all these numbers? Without human analysis, they are useless – as Paine says, "measurement without insight is just trivia."

As Paine outlines in her book, *Measuring Public Relationships: the Data-Driven Communicator's Guide to Success*, and presented at the 2009 WWPAS, there are several reasons to measure success. First, you look for failures and stop doing them, directing resources away from them. You keep abreast of what your competition is doing – in TRADOC's case, we like to compare our Websites and social media with the other two ACOMs, Army Material Command and Forces Command. We may even find some successes we didn't know about, comparing to what was happening last month, last quarter, or last year.

The baseline for measuring Websites and social media are inherent in Paine's seven steps:

1. Define the expected return. What do you want to be different within or involving your organization? Measure that change.
2. Gauge the investment in personnel that operating the Website and / or social media costs you.
3. Define your audience and how you impact them. Understand your role in getting your audience to do what you want them to do.
4. Define your key performance indicators: cost savings, efficiency, productivity, engagement, trust / corporate ethos, thought leadership, or message penetration, for example.
5. Define benchmarks.
6. Conduct research.
7. Analyze the research.

QUANTIFYING DATA

There are basic methods of measuring your Website. Ask your DOIM for the server log files, which will tell you how many visitors have been to your Website, how long they stayed, and where they came from. Or, purchase

prohibits acquiring, reporting, processing or storing information on persons or organizations not affiliated with DoD, except under the circumstances authorized in Paragraphs 6 and 7 when this information is essential to accomplish Army missions. However, Paragraphs 6 and 7 cover law-enforcement and civil-disturbance operations reasons; neither paragraph covers assessments of Website audiences. Since the assessment is authorized, and required, by DoD Web policy, if the assessment foregoes collecting PII, it would comply with AR 380-13.)

Also see Paragraph 2-3a(2) in the new AR 360-1 when it is published: All commanders will evaluate the effectiveness of PA projects, plans, and operations.

compete.com's services (you must have enough traffic to even surface there, however). Either way, you are trying to quantify three elements:

- **Output** – total opportunities-to-see (OTS), also known as Website visitors or “eyeballs.” These stats count a visitor every time anyone does a search, so most eyeball numbers are overstated, according to Paine. The leaders in the eyeball-counting industry for Websites are comScore, Compete, Alexa, and Nielsen NetRatings. (Xinureturns shows most of these leaders on its dashboard for you.) For instance, comScore's metric is based on total visits, average minutes per visit, average visits per visitor, and average visits per usage a day. To try and measure how engaged visitors are with your Website, check for the percentage of repeat visitors and the percentage of visitors who stay on a page for five minutes or more.
- **Outtake** – calculate the percent of change in awareness, percent of change in preference, or percent of change in people talking about your key messages. This could be indicated by an increase in the network surrounding your blog, for instance (such as an increase in backlinks or trackbacks).
- **Outcomes** – percent of change in downloads, percent of change in requests for information. Percent of people who register for something via a form, for instance.

Similar to Paine's outcomes, another possibility of measuring success is to calculate the ratio of visitors to interactivity, which is determined thus:

1. Count the number of requests for your site's homepage, its natural starting point for most visitors.
2. Find a page that has a form (a feedback form will do nicely) and count the number of requests for a page that comes after the form (often a thank-you page). This will enable you to count visits on an inner page as well as interactivity with your site. You may find one visitor in 100 fills out the form and submits it.
3. Track the total number of requests from Step 1 and the ratio of requests between Step 1 and Step 2.

Many PAOs are familiar with the “old-fashioned” media analysis. If you're going to measure the number of messages your organization has in the media (a clip analysis), we recommend that you evaluate news stories (messages) in both external and internal media. Our recommended benchmarks in compiling a clip analysis are:

- 30 percent of the articles are positive to your organization;
- No more than 6 percent are negative;
- 29 percent contain your organization's key messages.

Areas to analyze may include:

1. Volume of coverage – how much written or how many minutes aired.
2. Messages sent vs. messages placed – number of press releases, phone calls, interviews, etc., that resulted in actual coverage.
3. How often coverage accurately reflected key messages.
4. “Share of voice” (SOV) – evaluate against that of competitors.
5. Categorize by media outlet – audience characteristics.
6. Content of coverage – study sentences, graphs, stories.
 - a. Positive, negative, neutral?
 - b. Are specific themes featured or not?
 - c. What adjectives are used? What does this tell you about the coverage?
 - d. Was coverage news, editorial, letter to editor, feature story or other type?
7. Other variables in content analysis:
 - a. Circulation of publication;
 - b. Quality of publication;
 - c. Prominence of organization in story;
 - d. Prominence of article in publication;
 - e. Visual presentation – does the clip include photograph or graphic art?
 - f. Spokesperson – who is quoted? What percentage of your CG's quotes contains key messages?

Since we're all so heavily Web-driven now, in addition to the clip analysis, your research may include an on-line *image* or *ethos* analysis, such as gathering information on:

1. Information on subject and tone of on-line postings.
2. Location and author of postings.
3. Positive and negative issues.
4. "Share of voice" on usenet groups and commercial service forums.
5. Web traffic (hits) on the story about your organization.

If you're going to do clip analysis, a thorough analysis is important because it shows which messages are getting through and which are not; which media outlets and which reporters are favorable and which are unfavorable and why; which spokespeople are most effective at getting key messages across; and which approaches are most cost-effective.

We have a media-analysis "scorecard" available for you to adapt, if you wish, to track the things we've been discussing. It's set up for print media but can easily be customized for broadcast media. Since it is set up as a "blanket" (in landscape orientation), it isn't included in this *Guide* but is available in the *Guide*'s document library.

Even if you don't evaluate these precise things, you should consider establishing tools that gauge how people thought before they received your message and what they think after receiving your message to gauge how your message is being received. Feed results into a central database – what we'll call here an *integrated communications tracking system*. The first step in setting up this system is to define a single overall communication goal for your entire organization and identify key stakeholders, as outlined in Chapter 4. You adjust your system as your themes and messages adjust, of course.

A notional tracking system set up for TRADOC Public Affairs' CI activities is on the next page as an example.

If you're specifically gathering data on your *social-media engagements*, Paine recommends *monitoring recurring themes, complaints, and messages inherent in people's comments and conversation* about you. You may monitor this through Technorati, BlogLines, Sphere or Google Blog Search, for example, but a caveat: "Due to the limitations of automated content gathering, typically only about 10 percent will be relevant to the topic at hand," Paine says. Similar to the clip analysis discussed above, analyze:

- **Depth of coverage** – How many times was your organization mentioned within a posting?
- **Dominance** – Is the posting exclusively about your organization? Did the posting go into the TRADOC-related subject in-depth with many links, or is it just a passing mention?
- **Subject** – What is the primary topic of the posting?
- **Tonality** – Did the posting leave the reader more or less likely to think favorably of your organization / TRADOC?
- **Positioning on key issues** – Did the post discuss any of the key issues facing the Army / TRADOC, and if so, how did the poster position our organization? Beneficially or negatively?
- **Nature of posting** – Was the posting designed to solve a problem, or was it simply a rant? Who is being discussed or quoted: your CG or other command spokesperson, or a rank-and-file employee?

A popular way of quantifying data is the *dashboard*. Companies like iDashboards.com or Corda.com, for instance, specialize in them. (The example to the right was captured from iDashboards.com.) Website dashboards can include page visits, the percentage of repeat visitors, the percentage of visitors who stay on the page for five or more minutes, average "dwell time" (the length of time a visitor stays on the page), or other indications of *output*; the percentage of change, up or down, in backlinks or trackbacks to measure *outtake*; or the percentage of responses to a survey, compared to how many page visits the survey received, as a measure of



outcome. Then, of course, there are the user-assessment results themselves, which we'll discuss in the following section.

Pg. 57, Caywood

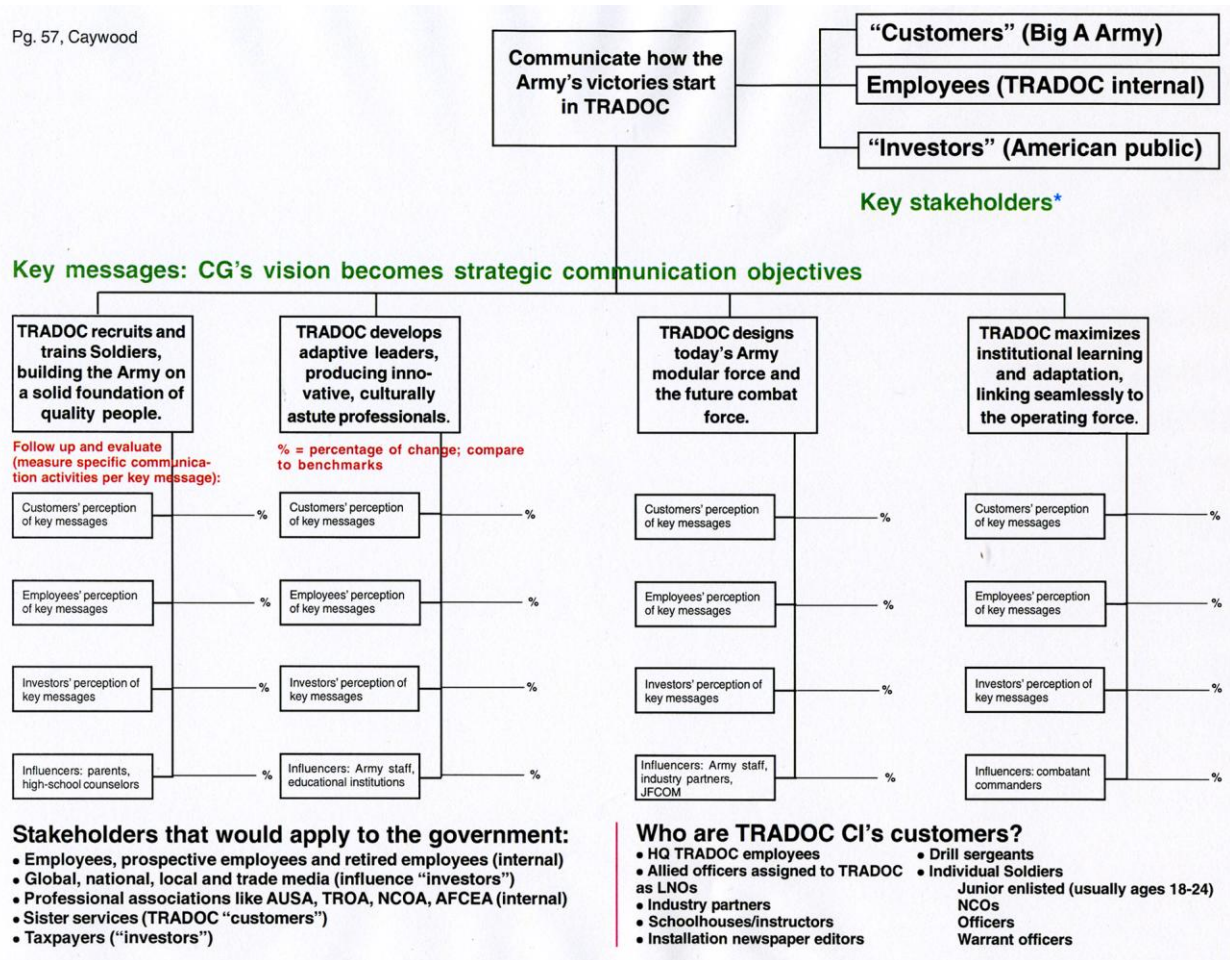
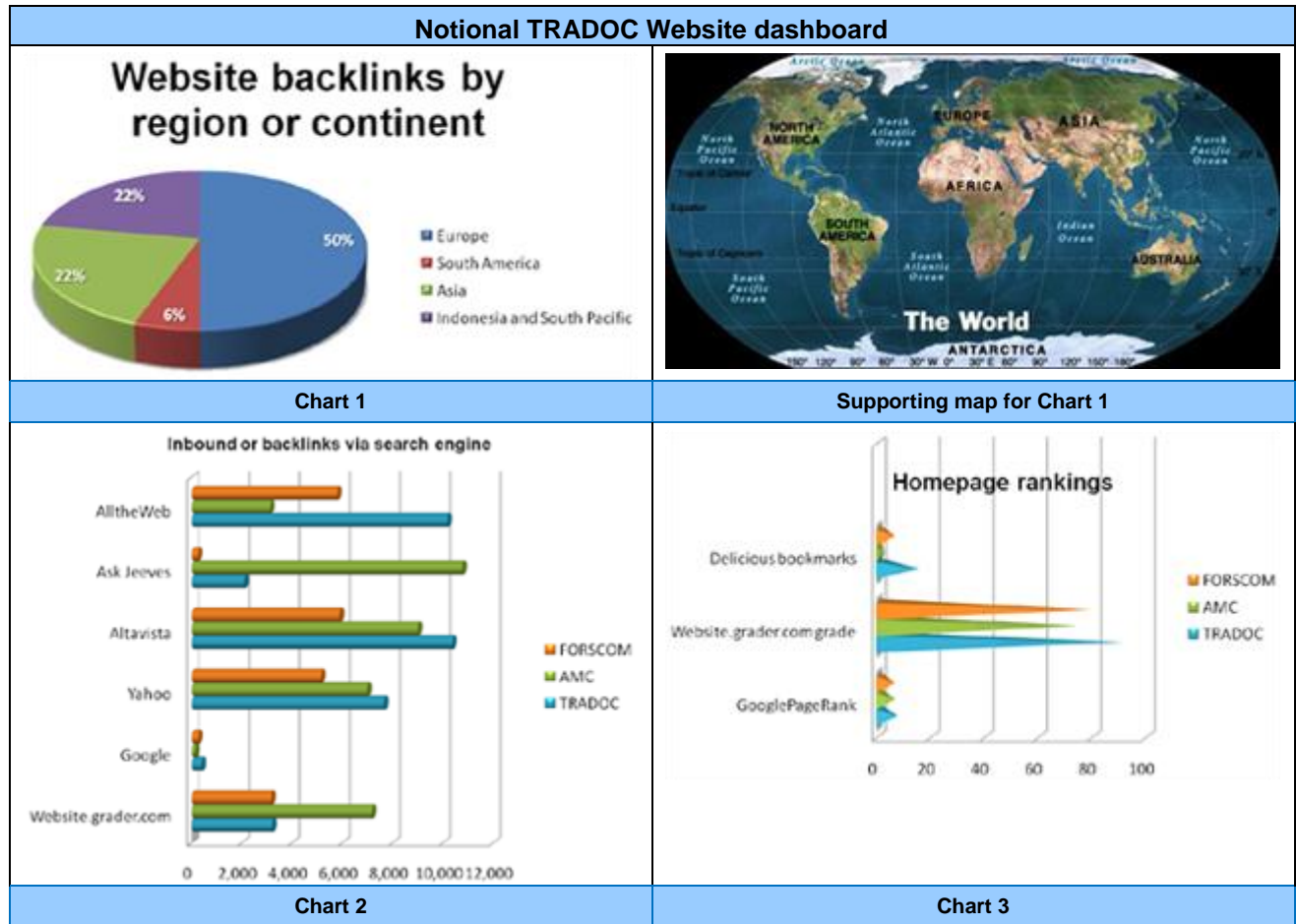


Chart O-1. The integrated communications tracking system designed for TRADOC PAO's CI section analyzes the impact of CI-generated stories supporting the TRADOC CG's vision and priorities.

Social media can be quantified via "audience reached through X program" types of analysis: the number of people who participate in Webchat, listen to a podcast, reply to a text message, receive a tweet, befriend a Facebook page, view a YouTube video, post a blog, etc. You may have several figures for these, such as number of people receiving text messages plus number of people replying to text messages.

Dashboarding is the latest enterprise effort in the knowledge-management community, including HQ TRADOC's knowledge-management offices. To show what kind of dashboard it's possible to build on statistics we can obtain free, we created the notional dashboard on the next page for the TRADOC Website. (All statistics were captured Aug. 23, 2009.)

We know it's mostly eye candy – remember, this is a *notional dashboard*. Google Analytics, although free, wants a verification email to sign up for an account, and we haven't been able yet to overcome the spam / junk email filters and blocks to get that account. Therefore the notional dashboard had to be built without Google Analytics. So, if we had Google Analytics or competite.com Pro, we'd analyze what pages people are visiting and how long they spend on those pages – in this notional dashboard, we analyzed backlinks, page rank, and unique visitors to check not only numbers but trends. We built charts in PowerPoint (with the exception of the unique Website visitor numbers and trends that competite.com calculated for us) – it was a definite do-it-yourself project. The point is that you can start simply and, as you gain more experience, your measurements, analysis, and measurement instruments get more sophisticated.



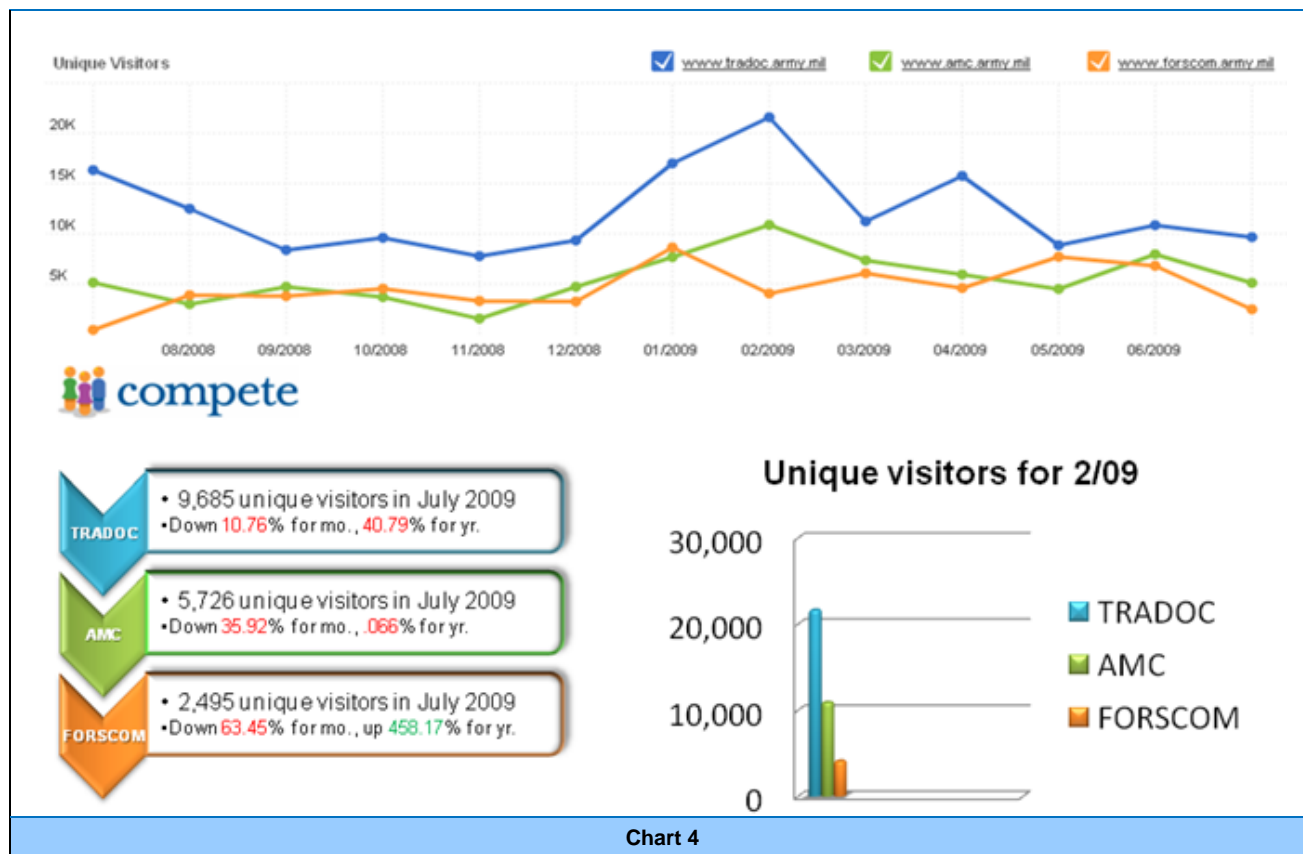


Chart 4

Backlinks. We studied backlinks – which are incoming links to a Website or Webpage and therefore are also known as in-bound links – on Charts 1 and 2. (The map beside Chart 1, which is present to orient our dashboard viewers geographically, would, most likely, be a link on a “real” dashboard – the dashboard compiler could provide a link, for instance, to a political map with all the countries drawn in, and could perhaps even provide the country names and link to their *CIA World Factbook* pages, which contain not only a map of the country but other interesting information.) Here we used backlinkwatch.com to check the TRADOC homepage, which told us we had 642 backlinks and gave us URLs for each backlink for further analysis. We discounted links from our own social-media sites, of course, and counted repeating domains as one backlink, although backlinkwatch.com counted them separately. **Backlinks can be a fairly suspect statistic**, so they have to be treated with a grain of salt. As an example, when we checked the TRADOC CG’s blog (TRADOC Live) for backlinks through backlinkwatch.com, the site said the blog had 509 backlinks. However, when we analyzed URLs, we saw there were only five unique backlinks. Someone had put us on their blogroll and showed us as a constant link from their blog’s left-side navigation, therefore each of their blog posts counted a backlink. The lesson-learned here is that you can’t count backlink numbers without analyzing how many are unique.

A similar term, *linkback* or *pingback*, is a method Web authors use to obtain notification when other pages link to one of theirs. Unlike backlinks, linkbacks are done via your own code programming. *Trackbacks*, a subset of linkbacks, is primarily used for connections to blogs. Be careful not to get *backlink* and *linkback* confused.

Knowing about in-bound links or backlinks is mostly useful to a Webmaster, and maybe not even a Webmaster so much since there is such a wide variation, as you’ll see on Chart 2. Chart 2 lets us know, however, that we need to continue to work with our Webmaster to enhance search-engine optimization.

One thing that caught our eye as we analyzed the backlinks’ URLs was what countries backlink to the TRADOC Website, which we could see by studying the top-level domain name. As Chart 1 shows, half the backlinks are from nine European countries: Germany, the United Kingdom, Switzerland, Spain, the Netherlands, Italy, the Czech Republic, Poland, and Hungary. There were four backlinks from Asian-continent domains: Japan, China, Taiwan, and the Russian Federation – and four from Indonesia and the South Pacific: Australia, New Zealand, Singapore, and Tokelau. At this time, we have one backlink from South America: Brazil. Depending on what we think is

useful to measure / know, we could easily modify this statistic and count all foreign backlinks separately to get a picture of how many times foreign backlinks come into the TRADOC site – again, we counted only unique domains, so no matter how many backlinks we had from Japanese URLs, for instance, Japan counted only once. Also, a statistic we could have counted with a bit more work (we would investigate the URLs’ destinations more thoroughly) was how many of the foreign backlinks were from those countries’ military Websites.

Since we want to measure where our Website visitors come from and, eventually, what they’re looking for, foreign backlinks (and any subset of those) can be a statistic. We can also analyze server logs for this information.

Page rankings. Chart 3 measures page rankings; grouped together as they are, it gives us a **snapshot of our corporate ethos**. For instance, TRADOC has 15 Delicious bookmarks, while TRADOC’s peers, the other two ACOMs, have two and six Delicious bookmarks, respectively. Delicious is a social-bookmarking Web service that enables users to store, share, and discover others’ Web bookmarks. Owned by Yahoo and with more than 5 million users, it’s nothing to sneeze at. Users choose their own index terms and may access their bookmarks via any Internet connection, including on their PEDs; if a site’s important enough to a user to bookmark, that says something.

[Website.grader.com](#) gave TRADOC’s Website a grade of 91, compared to AMC’s 74 and FORSCOM’s 79. This Website is a search-engine optimization tool, but two of the page-ranking sources that affect its grades are Google PageRank and Alexa. We’ll come back to Google PageRank, as we measured it separately in Chart 3. Alexa, an on-line service that measures site traffic, ranked TRADOC at 2,987 out of the millions of sites it checks, or in the top 0.01 percent.

Google PageRank’s ranking of TRADOC’s site is 7 on a scale of 1 - 10, while AMC and FORSCOM both garnered 6s. Google PageRank analyzes **link structures, which are an indicator of page value, which can be an indicator of Website value**. As [bloghubspot.com](#), sponsor of [Website.grader.com](#), observed, a link from Page A to Page B is a vote by A for B, and thus we get page rankings. “Google PageRank is an independent measure of Google’s perception of the quality / authority / credibility of an individual Webpage,” wrote [bloghubspot.com](#). Hubspot’s evaluation of page rankings is that 0-3 rankings on Google PageRank are usually new sites or sites with very minimal links to them. Ranks of 4 and 5 are popular sites with a fair amount of in-bound links, while 6 indicates very popular sites that have hundreds of links, many of them quality links (from sites that have high page rankings themselves). The 7-10 range, where TRADOC sits, usually includes media sites (e.g., [NYTimes.com](#)), big companies, or A-list bloggers, said Hubspot.

An **on-line survey would also give us an assessment of TRADOC’s corporate credibility and may paint a different picture**. The user assessment, required annually, is essentially a customer-satisfaction survey but may measure other things.

Unique visitors. The final chart in this notional dashboard is actually three charts. [Compete.com](#) provided the July 2009 numbers and even gave us the line graph we included at the top of Chart 4 that tracked the number of unique visitors – or first-time visitors – to our site over the past year. (You can check just your URL, or you can compare up to three other URLs to see how your peers / competitors are faring.)

Traffic numbers ebb and flow, and counting them is much like counting hits (how idiots track success, remember) – it’s the trends we wanted to capture, so we looked more closely at July’s statistics. We aren’t celebrating the fact that we had a larger amount of unique visitors for the month than our peers did, since we have a large continuing trend downward in the number of unique visitors per month. Of course, after that tremendous spike in unique visitors in February and a smaller one in April, a downward trend wasn’t unexpected. Still, a large amount of unique visitors plus a steady (like AMC) or rising (like FORSCOM) trend would be better. The trend shows that we need to work on our site content.

The TRADOC blog was not captured on this notional dashboard because the number-crunching was inconclusive. The TRADOC blog doesn’t register on blog-ranking sites such as Technorati. [Blog.grader.com](#) graded the blog at 55 out of 100; ranked it at 3,478 out of 7,906; and gave it an Alexa traffic rank of 282,622 – not so good as far as traffic measurement goes. However, [blog.grader.com](#) also counted its in-bound links at 855 (vs. [backlinkwatch.com](#)’s 509, of which only five were unique links); gave its Google PageRank as 6; and said it had one Delicious bookmark.

On the other hand, Paine says the better measurement of a blog’s success is the network surrounding the blog: the volume of conversations, comments, and trackbacks. Stowe Boyd, [stoweboyd.com](#), created the *conversation index*

for blogs, which tries to measure the degree to which a blog generates conversations. The **conversation index is the sum of comments made to a blog, plus trackbacks, divided by the total number of posts**. Paine says a conversation index of one or greater is acceptable.

If so, the TRADOC blog fares better. The blog presently has two comments and, since we can't check trackbacks, we substituted the number of unique backlinks, which as we said above was five as seen through the lens of backlinkwatch.com. (Counting trackbacks is more accurate than backlinks.) There are currently four posts, so seven divided by four equals a conversation index of 1.75.

THE ANNUAL SURVEY / USER ASSESSMENT

Much more useful, but much more work, is the Website user assessment or survey – required by Paragraph 8-2g, DA PAM 25-1-1, to be conducted annually. As we discussed in Chapter 4, it's the commander's / director's overall responsibility, but it's the organizational Website coordinator / post- or ACOM-level Web-content manager's responsibility to design and conduct on-line user-satisfaction surveys on the commander's / director's behalf. This **annual survey assesses satisfaction with the organization's or command's Website and includes these criteria at minimum**: the site's ease and consistency of use, or its navigability; what key messages were conveyed; how interactive users found the site; if users viewed the site's content as consistent; and how well integrated Website content is with the rest of the command's information products.

Conducting a survey of one's Website content is not for the faint of heart. No one in DoD or DA does them that we could find, so there's no precedent or "trailblazer" – there's only the policy that requires a survey. ARI does not administer them but does say that a Website "customer satisfaction" survey does not require OMB approval.⁶⁷⁰ There is no template for one in any DoD / DA policy document. OMB must approve any collection of standardized information from 10 or more persons – and obtaining OMB's approval can take up to six months. Part of that OMB-approval process is publication in the *Federal Register* of a notice to the public, plus a time period for public comment, of an organization's intent to collect information from the public. (At the end of this appendix, we show examples of notices published in the *Federal Register* pertaining to Website customer-satisfaction surveys.) Unless an organization avoids collecting PII, the survey must be IAW AR 380-13. Understandably, due to all these obstacles, most people do what they've always done: avoid conducting a Website-user assessment.

However, if you do want to endeavor doing the assessment yourself, the Institute for Public Relations has a comprehensive library of its research papers on measurement and evaluation at http://www.instituteforpr.org/research/measurement_and_evaluation/. Within the federal government, we must rely on the *Resource Manual for Customer Surveys* that OMB published in 1993. Ironically, OMB doesn't have the manual on its Website, but we found it in the "CyberCemetery," which is the partnership between the University of North Texas Libraries and U.S. Government Printing Office, as part of the Federal Depository Library Program, to provide permanent public access to the Websites and publications of "defunct U.S. government agencies and commissions." OMB's manual is in the crypt of the National Partnership for Reinventing Government (formerly called National Performance Review) at <http://govinfo.library.unt.edu/npr/library/omb.html> and is viewable in parts: Parts 1 through 7 are linked from this URL. (Slight edit: the Part 6 link is there but doesn't work. We're still looking for another source for Part 6.) However, a lot of what the Institute of Public Relations offers more than adequately covers what the manual includes. **Bottom line here: plan well ahead to conduct the annual assessment.**

A last recommendation: read the National Institutes of Health (NIH)'s paper at <http://www.jmir.org/2008/1/e4> for its account of how it administered an enterprise-wide Website-user assessment called the American Customer Satisfaction Index. NIH, part of the U.S. Department of Health and Human Services, wanted to better understand its Website users so it could ensure that its Websites were "user friendly and well designed for effective information dissemination" – precisely what TRADOC organizations should be measuring. NIH deployed the survey on a large number of its Websites – enough Websites that the survey could be considered "enterprise-wide" and probably the largest Web assessment of any kind, in the federal government. NIH, however, didn't do it as a do-it-yourself project. It created a program called the NIH Evaluation Set-Aside Program, kept the program in place for two years, spent \$1.5 million (\$1.275 million for survey licenses for 60 Websites at \$18,000 per Website) and hired a project-evaluation contractor for \$225,000. The contractor used the 10-point Likert scale rather than the typical five-point rating scale; standard questions from this study are included at the end of this appendix.

⁶⁷⁰ Per email from ARI dated July 22, 2009: "Evidently [the Defense Manpower Data Center], who owns the DoD survey business, has stated that customer-satisfaction surveys do not require an approval."

58368

Notices

Federal Register

Vol. 61, No. 221

Thursday, November 14, 1996

This section of the FEDERAL REGISTER contains documents other than rules or proposed rules that are applicable to the public. Notices of hearings and investigations, committee meetings, agency decisions and rulings, delegations of authority, filing of petitions and applications and agency statements of organization and functions are examples of documents appearing in this section.

AFRICAN DEVELOPMENT FOUNDATION

Sunshine Act Meeting; Board of Directors Meeting

TIME: 2:00–3:00 p.m. and 8:30–12:00 noon.

PLACE: ADF Headquarters.

DATE: Monday, November 18, 1996 and Tuesday, November 19, 1996.

STATUS: Open.

Agenda

Monday, November 18, 1996

2:00 p.m.—Chairman's Report

3:00 p.m.—President's Report

5:00 p.m.—Adjournment

Tuesday, November 19, 1996

8:30 a.m.—President's Report, Continued
12:00 noon—Adjournment

If you have any questions or comments, please direct them to Ms. Janis McCollim, Executive Assistant to the President, who can be reached at (202) 673–3916.

William R. Ford,

President.

[FR Doc. 96–29369 Filed 11–12–96; 3:32 pm]

BILLING CODE 6116–01–P

DEPARTMENT OF AGRICULTURE

Office of the Secretary

Request for Extension of a Currently Approved Information Collection

AGENCY: Office of the Secretary, Office of Chief Information Officer, United States Department of Agriculture.

ACTION: Notice and request for comments.

SUMMARY: In accordance with the Paperwork Reduction Act of 1995, this notice announces USDA's intention to request an extension of an information collection currently approved in support of customer satisfaction

surveys. Executive Order 12862 requires agencies and departments to identify and survey its "customers to determine the kind and quality of services they want and their level of satisfaction with existing service," and to "survey frontline employees on barriers to, and ideas for, matching the best in business" as part of the process of becoming customer focused. USDA is requesting generic approval to conduct a number of customer satisfaction surveys over the next 3 years.

DATES: Comments on this notice should be received on or before January 17, 1997 to be assured of consideration.

FOR FURTHER INFORMATION CONTACT: Larry K. Roberson, Department Clearance Office, Office of the Chief Information Officer, USDA, Mail Stop 7602, Washington, D.C. 20250; Telephone (202) 720–6204.

SUPPLEMENTARY INFORMATION:

Title: Customer Survey Activities.
OMB Control Number: 0505–0020.

Type of Request: Extension of a currently approved information collection.

Abstract: Executive Order 12862 requires Federal Departments to establish and implement customer service standards. This "Generic Clearance" encompasses all information collection activities within USDA that will be conducted in order to satisfy the requirements of the Executive Order.

Estimate of Burden: Public reporting burden for this information collection is estimated to average 15 minutes per response.

Respondents: Individuals or households; State or local government; Farms; business or other for-profit; Federal agencies or employees; Non-profit institutions; Small businesses or organizations.

Estimated number of Respondents: 200,000.

Estimated number of Responses per Respondent: 1.

Estimated Total Annual Burden on Respondents: 50,000 hours.

Comments regarding: (a) whether the collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility; (b) the accuracy of the agency's estimate of burden including the validity of the methodology and assumptions used; (c) ways to enhance the quality, utility and clarity of the

information to be collected; (d) ways to minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques should be sent to Larry Roberson at the above address.

All responses to this notice will be summarized and included in the request for OMB approval. All comments will also become a matter of public record.

Signed at Washington, DC, on November 7, 1996.

Larry K. Roberson,

Deputy Departmental Clearance Officer.

[FR Doc. 96–29108 Filed 11–13–96; 8:45 am]

BILLING CODE 3410–01–M

Submission for OMB Review; Comment Request

November 8, 1996.

The Department of Agriculture has submitted the following information collection requirement(s) to OMB for review and clearance under the Paperwork Reduction Act of 1995, Public Law 104–13. Comments regarding these information collections are best assured of having their full effect if received within 30 days of this notification. Comments should be addressed to: Desk Officer for Agriculture, Office of Information and Regulatory Affairs, Office of Management and Budget (OMB), Washington, D.C. 10503 and to Department Clearance Officer, USDA, OCIO, Mail Stop 7602, Washington, D.C. 20250–7602. Copies of the submission(s) may be obtained by calling (202) 720–6204 or (202) 720–6746.

• Agricultural Marketing Service

Title: Handling of Oranges, Grapefruit, Tangerines, and Tangelos Grown in Florida.

Summary: Information collected under Marketing Order 905 includes background statements for committee members, crop prospects, and requests for special purpose shipments.

Need and Use of the Information: The Citrus Administrative Committee needs specific information from handlers to monitor compliance, to develop a seasonal marketing policy and annual report, and statistics. This information

Sample O-2. The Department of Agriculture's **Federal Register** notice (required by law) starting in the left-hand column is a request for an extension of a previously approved request. Note the format; it is specific. OMB approval (and its control number) must be provided for the **Federal Register** notice.

FR Doc E9-11194

[Federal Register: May 13, 2009 (Volume 74, Number 91)]
[Notices]
[Page 22600]
From the Federal Register Online via GPO Access [wais.access.gpo.gov]
[DOCID:frl3my09-93]

=====

OFFICE OF PERSONNEL MANAGEMENT

Comment Request for Review of Information Collection: Agency
Generic Survey Plan OMB 3206-0236

AGENCY: Office of Personnel Management.

ACTION: Notice.

SUMMARY: In accordance with the Paperwork Reduction Act of 1995 (Pub. L. 104-13, May 22, 1995), this notice announces that the Office of Personnel Management (OPM) intends to submit to the Office of Management and Budget a request for review of a revised information collection. The agency Generic Survey Plan is an umbrella for all OPM customer satisfaction surveys used to measure satisfaction with OPM programs and services. This Plan satisfies the requirements of Executive Order 12862 and the guidelines set forth in OMB's "Resource Manual for Customer Surveys".

The information collection was previously published in the Federal Register on March 14, 2008, at 73 FR 13925 allowing for a 60-day public comment period. No comments were received on this existing information collection. The purpose of this notice is to allow an additional 30 days for public comments. Comments are particularly invited on: Whether this information is necessary for the proper performance of functions of OPM, and whether it will have practical utility; whether our estimate of the public burden of this collection of information is accurate and based on valid assumptions and methodology; and ways in which we can minimize the burden of the collection of information on those who are to respond, through the use of appropriate technological collection techniques or other forms of information technology.

The collections will include web-based (electronic), paper-based, telephone and focus groups surveys. We estimate approximately 1,000,000 surveys will be completed annually. The time estimate varies from 3 minutes to 2 hours to complete with the average being 15 minutes. The annual estimated burden is 250,000 hours.

DATES: Comments on this proposal should be received within 30 calendar days from the date of this publication.

ADDRESSES: Send or deliver comments to: OPM Desk Officer, Office of Information and Regulatory Affairs, Office of Management and Budget, New Executive Office Building, 725 17th Street, NW., Room 10236, Washington, DC 20503.

Please provide your mailing address or Fax number with your request.

Office of Personnel Management.
John Berry,
Director.

[FR Doc. E9-11194 Filed 5-12-09; 8:45 am]

BILLING CODE 6325-47-P

Sample O-3. The Office of Personnel Management (OPM) routinely outlines on the Internet its plans for information collection. Here its Website customer-satisfaction survey intentions are included in its generic survey plan. By law, 30 days are required for public comments on a proposed information collection; a Website survey must be planned well in advance just to accomplish it annually, as required.

Category	Question
	Please rate the following on a 10-point Likert scale.
	1 = poor, 10 = excellent
Site Performance	Speed of loading the page on this site? Consistency of speed on this site? Reliability of site performance on this site?
Search	Usefulness of search results on this site? Provides comprehensive search results on this site? Organization of search results on this site? Search features help you narrow the results on this site?
Privacy	Ability to limit sharing of your personal information on this site? Amount of personal information you are asked to submit on this site? Site's commitment to protecting your personal information?
Navigation	Number of steps to get where you want on this site? Ability to find information you want on this site? Clarity of site map or directory? Ease of navigation on this site?
Look and Feel	Ease of reading this site? Clarity of site organization? Clean layout on this site?
Functionality	Usefulness of the information provided on this site? Convenience of the information on this site? Ability to accomplish what you wanted to on this site?
Content	Accuracy of information on this site? Quality of information on this site? Freshness of content on this site?
	1 = very low, 10 = very high
Satisfaction	What is your overall satisfaction with this site? How well does this site meet your expectations? How does this site compare to your idea of an ideal Website?
	1 = very unlikely, 10 = very likely
Primary Resource	How likely are you to use this site as your primary resource for health information?
Recommend	How likely are you to recommend this site to someone else?
Likelihood to Return	How likely are you to return to this site?

Sample O-4. The above standardized questions are taken from the American Customer Satisfaction Index on-line customer survey that NIH conducted. Visit the URL previously listed for more details about the study.

Appendix P

IO and Public Affairs

As the PAO's skill set continues to change – whether officer or civilian – the line between Public Affairs and IO continues to blur in commanders' and the public's minds. (And yes, there must be a line; we'll come back to that.) Maj. Gen. Kevin Bergner, the Army's CPA, said at the 2009 Worldwide Public Affairs Symposium (WWPAS) that his vision is to have the Army story ever-present, compelling, and naturally credible. To do this, he said, the career field must transition to "Public Affairs operators." As Bergner described the Public Affairs operator, that individual is naturally offense-oriented, risk-tolerant, a competitor, integrated in the staff, and has expert knowledge from other sources (he / she is not limited by MTOE / TDA). The Public Affairs operator has skills in Public Affairs, IO, and "pol-mil."

There's a necessary skill Bergner didn't mention: the ability to diplomatically walk the line between IO⁶⁷¹ and the legally defined role of Public Affairs. Public Affairs is considered **one of the supporting and related capabilities** to IO. (E.g., "IO-related activities include ... Public Affairs."⁶⁷²) However, Public Affairs has a legal and doctrinal role that cannot cross into IO.⁶⁷³ As the DoD IG states in its Dec. 10, 2008, report on the ASD-PA (report D-2009-028), Public Affairs is the official public spokesperson and information-release authority, and oversees the performance of such functions as:

- Developing DoD Public Affairs policies, plans, and programs;
- Ensuring the free flow of news and information;
- Planning, programming, and budgeting activities; and
- Responding to inquiries on DoD policies, programs, and activities.

Also, as we detailed have detailed in this *Guide*, Public Affairs as a content provider is the commander's principal adviser for news-media relations, public liaison, internal communications, community relations, audiovisual matters, and Public Affairs and VI training.⁶⁷⁴

We've strayed from our defined roles, and that may be detrimental to not only our Public Affairs career field, but ultimately to the Army. The DoD IG's report included discussion on two important documents:

- "DoD [JP] 3-61, **Public Affairs**, May 9, 2005, states that Public Affairs and [IO] functions should directly support military objectives, counter adversary disinformation, and deter adversary actions. The publication also states that although Public Affairs and the [IO] functions require planning, message development, and media analysis, the **efforts differ with respect to the audience, scope, and intent, and must remain separate. The publication further states that commanders should structure their organizations to ensure the separation of Public Affairs and [IO].**"⁶⁷⁵
- "[DoDD 3600.1], **Information Operations**, Aug. 14, 2006, recognizes the need for [IO] to use Public Affairs products and information to communicate military objectives, counter misinformation and disinformation, deter adversary actions, and maintain the trust and confidence of the U.S. population. However, the directive assigns the Under Secretary of Defense (Policy) the responsibility to establish specific policy and oversight for the development and integration of [IO] and coordinate with the Under Secretary of Defense (Intelligence) and the ASD(PA) for establishing specific policy and oversight for the development and integration of public diplomacy as a related [IO] capability. Assigning the [Deputy ASD] for Joint Communication the responsibility for synchronizing Public Affairs and [IO] allows for the **improper integration** of these functions."⁶⁷⁶

⁶⁷¹ Defined in FM 3-13 as the "integrated employment of the core capabilities of electronic warfare, computer network operations, [PSYOP], military deception, and [OPSEC], in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making while protecting our own."

⁶⁷² Paragraph 1-58, FM 3-13.

⁶⁷³ For instance, IAW Paragraph 3-1f, AR 360-1: "[PAOs] and their staffs will not initiate or conduct psychological or deception operations and will not permit PA resources to be used to support such activities."

⁶⁷⁴ Paragraph 3 and Enclosure 2, DoDD 5122.05; Paragraphs 2-4 and 5-2, AR 360-1.

⁶⁷⁵ Page 11, DoD IG Report D-2009-028, <http://www.dodig.mil/Audit/reports/fy09/09-028.pdf>.

⁶⁷⁶ Page 12, DoD IG Report D-2009-028.

The Senate, in its June 2007 report on the Fiscal Year (FY) 2008 National Defense Authorization Act, articulated that Public Affairs should not be integrated with IO: “Responsibility for strategic communication and public diplomacy rests with the President and Secretary of State, and any DoD efforts to formulate a message should be informed and framed by those efforts. Moreover, public diplomacy, public affairs, and [IO] are separate and distinct functions, with different purposes and guidelines for their use. Any attempt to integrate them could compromise the integrity of each of these functions.”⁶⁷⁷

Rep. Ike Skelton, chairman of the House Armed Services Committee, emphasized that Public Affairs and IO were distinct in his speech at the 2009 WWPAS.

The DoD IG’s report cautioned that “[w]ithout clearly defined strategic-communication responsibilities, DoD may appear to merge inappropriately the Public Affairs and [IO] functions. The OASD(PA) should only perform strategic-communication responsibilities related to its Public Affairs mission. The strategic-communications responsibilities for [IO] should remain separate and under the oversight of the Under Secretary of Defense (Policy).”⁶⁷⁸

So how do you do strategic-communications planning anymore without getting into hot water? Dovetailing onto our discussion in Chapter 4 of “strategic Webbing,” practicing strategic messaging on the Web IAW these concepts is different in nuance and results than strategic communication as the Army practices it. Our concepts are closer to Wikipedia’s definition of strategic communication: “Strategic-communication management is defined as the systematic planning and realization of information flow, communication, media development, and image care in a long-term horizon. It conveys deliberate message(s) through the most suitable media to the designated audience(s) at the appropriate time to contribute to and achieve the desired long-term effect. Communication management is process creation. It has to bring three factors into balance: the message(s), the media channel(s), and the audience(s).”⁶⁷⁹

As Professor Dennis Murphy of the U.S. Army War College said in his thought-provoking article, “The Trouble with Strategic Communication,” no one in the military really knows what strategic communication is – therefore it is meshed into IO. “There is no overarching U.S. government definition of strategic communication,” Murphy wrote. “There is, however, a [DoD] definition as a result of the most recent [QDR] [Feb. 6, 2006], which produced a Strategic Communication Roadmap. Strategic communication is ‘focused USG processes and efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable to advance national interests and objectives through the use of coordinated information, themes, plans, programs, and actions synchronized with other elements of national power.’ The Roadmap goes on to list the primary supporting capabilities of strategic communication as Public Affairs, aspects of [IO] (principally psychological operations), military diplomacy, defense support to public diplomacy, and visual information. Unfortunately this list limits the perceived means available to communications-based activities and so reinforces the lexicon of the term itself. And therein lies the rub with current interpretations of strategic communication by military leaders. Considering strategic communication as a menu of self-limiting communications capabilities will ensure the plane never takes off.”⁶⁸⁰

The lack of clarity on strategic communication, we think, is what led to the DoD IG’s criticism of Public Affairs and the resulting public comment. In the article, “Costs of PR rise and raise propaganda flag,” included in the *Virginian Pilot* Feb. 6, 2009, journalist Chris Tomlinson of the Associated Press (AP) reported that the Pentagon had “dramatically” increased its expenditures to “win the human terrain of world public opinion.” Tomlinson reported on an AP investigation that lumped Public Affairs with recruitment and advertising, calling it all “PR,” and said that in the past five years, the military had spent 63 percent more – at least \$4.7 billion – on PR. Tomlinson also said that \$547 million of the Pentagon’s budget goes to Public Affairs, “which reaches U.S. audiences,” and that spending on Public Affairs has more than doubled since 2003.

“Recruitment and advertising are the only two areas where Congress has authorized the military to influence the American people,” Tomlinson wrote. “Far more controversial is public affairs, because of the prohibition on domestic propaganda.”

⁶⁷⁷ Page 10, DoD IG Report D-2009-028.

⁶⁷⁸ Page 11, DoD IG Report D-2009-028.

⁶⁷⁹ From http://en.wikipedia.org/wiki/Strategic_Communication.

⁶⁸⁰ From http://www.army.mil/professionalwriting/volumes/volume6/september_2008/9_08_2.html.

*Influence*⁶⁸¹ undoubtedly means something different to the commercial media than it does to Army IO practitioners, but we also doubt that the article is unbiased since it pointedly merges “domestic propaganda” with Public Affairs. Tomlinson wrote that “[PAO] may have crossed the line into propaganda. The audit found [DoD] ‘may appear to merge inappropriately’ its public affairs with operations that try to influence audiences abroad. It also found that while 89 positions were authorized for public affairs, 126 government employees and 31 contractors worked there.”

Tomlinson’s article is somewhat disingenuous, however, as the DoD IG report discusses the organization of OASD-PA – it does not cover the practice of Public Affairs – and it does not say that PAO “crossed the line into propaganda” but that some functions were improperly merged under one supervisory chain. What the DoD IG report said about ASD-PA’s manning was that the “manpower document, dated [Sept. 4, 2007], authorized 89 OASD(PA) positions. In July 2007, the Special Assistant to the ASD-PA conducted an evaluation and ... determined that at least 109 government and 31 contract employees worked directly for the OASD-PA.”⁶⁸² Anyone who’s been around the military for any length of time knows that authorizations and manning don’t always match; the numbers ebb and flow with factors such as rotations and hiring. So we can’t know how to interpret the ASD-PA’s manning numbers, but we doubt that they’re doing anything sinister vis a vis “domestic propaganda.” What they have done – and this is how Public Affairs became linked with IO – is muddy the waters a bit on strategic-communication funding sources.

DoD Public Affairs has a deputy ASD (DASD) for Joint communication, a position undefined by DoDD 5122.5 – a DoDD we have previously mentioned in this *Guide* as specific to the ASD-PA but one containing principles all DoD PAOs can apply. “The [QDR] identified gaps in the primary supporting capabilities of Public Affairs, defense support to public diplomacy, military diplomacy, and [IO] and psychological operations,” said the DoD IG report. Because of the QDR, the DEPSECDEF developed a strategic-communication execution roadmap (referred to by Murphy) and established the Strategic Communication Integration Group (SCIG). The DEPSECDEF appointed the DASD for Joint communication as the SCIG secretariat director.⁶⁸³ At that time, the funding lines began to criss-cross between Public Affairs and strategic communication, which the DoD IG report outlined.

Funding-line blurring may seem par for the course to long-time DoD employees, but it’s not so innocuous to the civilian media, apparently. Tomlinson quoted Robert Hastings, acting director of DoD Public Affairs, about the increase in the “PR” budget: “Hastings says the growth reflects changes in the information market and the fact that the United States is now fighting two wars. ‘The role of Public Affairs is to provide you the information so that you can make an informed decision yourself,’ Hastings says. ‘There is no place for spin at [DoD].’”

We point this out because of the possible “spin” in an article about perceived DoD spin. One, if we don’t keep our lines of operation clear, indeed we may stray organizationally, albeit unintentionally, into IO. Two, if we don’t keep our operations “pure” Public Affairs, the public loses respect and trust in Army Public Affairs. We end up with congressional leaders like Rep. Paul Hodes, a Democrat from New Hampshire, saying, “It’s not up to the Pentagon to sell policy to the American people” (as quoted by Tomlinson), but worse, the Army must deal with perceptions like Hodes’ – who not only holds the perception of military wrong-doing but acted upon it, sponsoring legislation last year reinforcing the ban on “domestic propaganda.”

We predict that the public discussion will begin again as the Army considers, via conferences this summer, lumping Public Affairs together with PSYOPS, at minimum, under the heading *military public relations*. The lines between Public Affairs and propagandizing will blur more if the Army moves from concept to practice on this.

Respect and credibility for PAO practitioners and the Army are hard-won, easily lost, and critical. Truth is paramount.⁶⁸⁴ So is the perception of truth-telling and straightforwardness. Secretary of the Army Pete Geren addressed this when he said at the 2009 WWPAS: “We win with transparency. We lose when getting information out of us is like pulling a molar. ... Bad news does not get better with time.

“The Army is the best institution, purest of heart, a force for good in the world of any I’ve been associated with, but we do make mistakes. We’re going to be honest when we make a mistake and lay it out there,” Geren said.

⁶⁸¹ *Influence*, as defined in Paragraph 1-62, FM 3-13, is “to cause adversaries or others to behave in a manner favorable to Army forces.”

⁶⁸² Page 14, DoD IG Report D-2009-028.

⁶⁸³ Page 10, DoD IG Report D-2009-028.

⁶⁸⁴ Paragraph 2-107, FM 3-13.

The Army's truth-telling must stand against media bias. As Jamie McIntyre, former Cable News Network (CNN) senior Pentagon correspondent, said, "TV news is looking for things that make people outraged." We could apply that to other forms of mainstream media as well.

The Army's truth-telling must also persevere in an environment of changing information sources. As Tom Curley, president and chief executive officer (CEO) of AP, said at the 2009 WWPAS, an AP poll of mainstream-media journalists revealed that three-fourths of them read one or more blogs, and one-third of them read five or more blogs weekly. Not only do journalists read blogs for news sources, but blog readership is up among Internet users – blogs themselves have become news sources for Internet users. Curley said that there were two key aspects to this change: 1) modern devices (i.e., Blackberry, iPod, or Really Simple Syndication, or RSS, feeds) make it possible to be your own editor, so people are not depending on the traditional media to be the "gatekeeper"; and 2) 46 percent of population consumes news, leading to a news boom, but they're not going to the traditional media for news. This has some implications for Public Affairs' efforts to speak with "one voice."

Public Affairs and strategic-communication as we describe (which would adhere to the DoD IG's statement that Public Affairs "should only perform strategic-communication responsibilities related to its Public Affairs mission") – and coordination with the staff but a delineation / separation in function – must be the Army's constant practice. Public Affairs should not be under an IO cell / command or lumped under "military public relations" but be directly on the commander's personal staff as the command's spokesperson – and the person / office the public pinpoints for queries about the command.

And so Public Affairs must walk a thin line regarding information engagement⁶⁸⁵ (described in Chapter 7, FM 3-0), as its public-domain activities (discussed in the first four chapters in this *Guide*) are built on the concepts that the Army's public-engagement efforts serve the public's needs, including using new technologies to place information about the Army's operations and decisions on-line, where it is readily available to the public. We find out what information is of greatest use to the public by soliciting public input. In a sense, Army Public Affairs fulfills a collaborative function with the public, identifying through analysis and public feedback ways to improve our cooperation with the public.⁶⁸⁶ In doing these things, Army Public Affairs executes functions of government, not just necessities of the military, as IO does. IO, in the words of Lt. Col. Eric Henderson of CAC's IO Proponent at Fort Leavenworth, Kan., "is about command-and-control warfare – it is not, and never has been, about building collaboration."⁶⁸⁷

The DoDI on Public Affairs operations requires that DoD Public Affairs and IO "be coordinated to optimize effects and the achievement of DoD goals,"⁶⁸⁸ but that doesn't mean integration. The DoDI, in fact, charges intelligence senior leaders to coordinate with Public Affairs on developing and implementing policy for the coordination, synchronization, and *deconfliction* of IO and Public Affairs.⁶⁸⁹ Even the IO FM, FM 3-13, acknowledges Public Affairs' relationship with the American public: "Effective Public Affairs truthfully informs the public. It does not focus on directing or manipulating public actions or opinion."⁶⁹⁰ [Public Affairs] fulfills the Army's obligation to keep the American people and the Army informed. It helps establish conditions that lead to confidence in the Army and its readiness to conduct operations during peace, crisis, and war. PA keeps all members of the force informed."⁶⁹¹

IO use of Public Affairs' products to "counter the effects of adversary propaganda and misinformation" is expected (at least in DoDD 3600.1), but it is still coincidental – ergo, Public Affairs does not prepare products especially for use by the IO community. And it is also somewhat dangerous – if Public Affairs is identified as the source of IO material, Public Affairs is accused of "spin," "propaganda," or other inappropriate uses of information – but there seems to be no good answer for this other than to continually message that Public Affairs is distinct and separate, (and, in actuality, keep those lines of demarcation distinct and separate).

⁶⁸⁵ Defined in FM 3-0 as "The integrated employment of Public Affairs to inform U.S. and friendly audiences; [PSYOP], combat camera, U.S. government strategic communication and defense support to public diplomacy, and other means necessary to influence foreign audiences; and, leader and Soldier engagements to support both efforts."

⁶⁸⁶ Based on the presidential memo, "Transparency and Open Government, Jan. 21, 2009, http://www.whitehouse.gov/the_press_office/Transparency_and_Open_Government.

⁶⁸⁷ From his presentation at the 2009 WWPAS.

⁶⁸⁸ Paragraph 4e, DoDI 5400.13.

⁶⁸⁹ Paragraph 2a, Enclosure 2, DoDI 5400.13.

⁶⁹⁰ Paragraph 2-102, FM 3-13.

⁶⁹¹ Paragraph 2-105, FM 3-13.

In the end, what Public Affairs does is conduct media-relations, community-engagement and command-information programs; maintain command-sponsored publicly accessible Websites; and “live” DoD’s principles of information.⁶⁹² That isn’t IO, and it isn’t necessarily strategic communication. It’s finding ways for truth-telling.

⁶⁹² Paragraph 6b, DoDI 5400.13.